



# Cybersecurity for Manufacturing Networks

---

*a White Paper prepared by*

**The NDIA Cybersecurity for Advanced Manufacturing  
Joint Working Group (CFAM JWG)**

**October 2017**

---

DISCLAIMER: The ideas and findings in this report should not be construed to be official positions of any of the organizations listed as contributing members of this Joint Working Group or the membership of NDIA. It is published in the interest of information exchange between Government and Industry, pursuant to the mission of NDIA.





## EXECUTIVE FOREWORD

In May 2014, the National Defense Industrial Association (NDIA) presented to the Undersecretary of Defense (Acquisition, Technology & Logistics) a report highlighting an emerging threat to U.S. national security. This threat stems from actions by nations and individuals exploiting cybersecurity weaknesses inherent in networked industrial control systems on shop floors of defense contractors and suppliers.

These cyber-attacks against the defense industrial base (DIB), where our military's equipment is produced, have significant national security implications. The 2014 report investigated the nature and scope of the threat and offered recommendations for mitigating the impacts of cyber-attacks on manufacturing networks.

As a follow-on action, with cooperation and support from several Office of the Secretary of Defense (OSD) organizations, NDIA formed a joint working group charged with providing specific ideas for implementing the recommendations in the original report and developing a coordinated approach across government agencies to address this rapidly escalating problem.

The Cybersecurity for Advanced Manufacturing Joint Working Group (CFAM JWG) focused on the protection of manufacturing networks from cyber-attacks in the defense industrial base where intensifying cyber-espionage calls for an urgent response.

The group identified ways for the Department of Defense (DoD) and its prime contractors to assist manufacturers, particularly small and medium enterprises (S&MEs) to improve cybersecurity by implementing evolving policies and contract requirements, enhancing security practices, developing technologies, and offering workforce cybersecurity training.

The recent release of Presidential Executive Order 13806 "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States" (21 July 2017) makes this White Paper both timely and appropriate. NDIA is proud to offer this study to assist the DoD and the manufacturing industry in securing the nation's manufacturing infrastructure from cyber-attacks and cyber espionage, and to engage in further activity that enables better protection of important national assets.

Herbert J. Carlisle  
General, USAF (Ret)  
President and CEO

(This page intentionally blank)



## PAPER DISPOSITION

This paper is formally submitted to the Undersecretary of Defense for Acquisition, Technology and Logistics. Permission is granted to widely distribute and quote with proper attribution. The 2014 White Paper was presented to, and accepted by, the USD AT&L.

## PRINCIPAL CONTRIBUTORS

NDIA appreciates the effort its member companies expended on this joint white paper with the Office of the Undersecretary of Defense for Acquisition, Technology and Logistics. The large number of experts who contributed to this effort are found in the list of CFAM members, page vi.

NDIA recognizes that an effort such as this cannot be completed without persons who take responsibility for its success and guide it from beginning to end. NDIA thanks and commends the following for their leadership and dedication:

### Chairperson

- Ms. Catherine Ortiz, Defined Business Solutions LLC, Chairperson of the JWG

### Senior Advisors

- Dr. Vicki Barbur, MITRE
- Dr. Larry John, Analytic Services Inc.
- Dr. Michael McGrath, McGrath Analytics, Chair of the original study
- Mr. Chris Peters, The Lucrum Group
- Ms. Anitha Raj, ARAR Technology
- Ms. Rebecca Taylor, The National Center for Manufacturing Sciences

### Team Leaders

- Dr. Marilyn Gaska, Lockheed Martin Corporation
- Ms. Heather Moyer, Crossroads Consulting LLC
- Ms. Sarah Stern, Boeing, Boeing Commercial Aircraft Network Cyber Security

NDIA also recognizes the engagement and guidance given by the following representatives from DoD, without whose interest and support this paper would not be possible:

- Mr. Donald Davidson, Office of the Department of Defense Chief Information Officer
- Mr. Robert Gold, Office of the Deputy Assistant Secretary of Defense for Systems Engineering
- Ms. Adele Ratcliff, Office of Manufacturing and Industrial Base Policy (MIBP)
- Ms. Melinda Reed, Office of the Deputy Assistant Secretary of Defense for Systems Engineering

## COPIES AVAILABLE FOR DOWNLOAD

This paper along with the predecessor paper, *Cybersecurity for Advanced Manufacturing*, May 5 2014, are available on the NDIA website (<http://www.ndia.org/divisions/working-groups/cfam>) as a reference resource.

(This page intentionally blank)

## EXECUTIVE SUMMARY

In 2014, the National Defense Industrial Association (NDIA) published a White Paper, “Cybersecurity for Advanced Manufacturing,” documenting the growing threat to manufacturing posed by cyber-attacks and offering recommendations for improving the security of manufacturing processes. Since then, the threat has grown in both scale and potential for damage. In 2015, the NDIA organized the Cybersecurity for Advanced Manufacturing Joint Working Group (CFAM JWG), consisting of members of industry, government agencies, academia, and research organizations, to implement the recommendations from the 2014 report and recommend further actions to develop an effective risk management program. Their findings and recommendations are reported in this 2017 White Paper.

The U.S. manufacturing industry, long a bulwark of the nation’s economic strength, is experiencing a rapid global trend toward digital manufacturing and advanced interconnectivity fueled by the Internet of Things (IoT) and the growing value of data, “the digital thread”, that traverses a manufacturing network. As this connectivity increases, malicious actors are developing more sophisticated ways to infiltrate manufacturing systems through a variety of hacking techniques. An increasing arsenal of cyber-attack tools is available to individuals, organized crime, and nation states, further elevating the risk. Denials of service, ransomware incidents, theft of intellectual property and destruction of facilities have already occurred. Between 2014 and 2016 the number of cyber-attacks against the nation’s critical manufacturing sector nearly doubled<sup>1</sup> due to the increasing attractiveness of the data traveling through manufacturing networks and the relative ease with which these networks can be penetrated.

The implications for the nation’s defense are alarming: adversary cyber-attacks on any manufacturing network can jeopardize product integrity, steal sensitive intellectual property (IP), and threaten production availability and safety. Coordinated attacks can damage entire industries or target supply chains that produce material critical to building and sustaining our military’s weapon systems. For defense systems, cyber-espionage can provide an adversary with the ability to leapfrog their existing capabilities and, more importantly, to develop countermeasures to U.S. technologies.

A stronger, more resilient, and more flexible cybersecurity risk management process is needed for the nation to have confidence that the U.S. manufacturing capacity will meet defense and economic security needs. Developing effective risk management processes has been hampered by lack of a clear understanding of the differences in the priorities of Information Technology (IT) and Operational Technology (OT). Unlike IT environments, OT networks are not highly adaptable and the impacts of attacks can be more acute: tampering can lead to safety systems failures or unreliable products—both with life-threatening consequences—and the loss of IP can diminish our technology superiority.

Creating effective solutions to improve cybersecurity is not solely a matter of concern for the Department of Defense (DoD). In fact, as Presidential Executive Order 13806 “Assessing and

---

<sup>1</sup> Corey Bennett, “DHS: Cyberattacks on Critical Manufacturing Doubled in 2015” *The Hill*; 15 January 2016. <http://thehill.com/policy/cybersecurity/266081-dhs-critical-manufacturing-cyberattacks-have-nearly-doubled>

Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States,” (July 2017) indicates, many government agencies have a stake in a secure manufacturing system. Some agencies are directly involved with manufacturing firms; others are charged with securing the nation’s economic infrastructure and providing defense against attacks by foreign governments and non-state actors. Hence, each organization can and should play a role in preventing cyber-crime, cyber-terrorism, and cyber-warfare and in helping build a manufacturing system in which vulnerabilities are minimized while operating efficiency is maintained or improved.

Some solutions have already been developed and are being implemented. The government instituted contract requirements to protect controlled unclassified data. Nevertheless, these requirements were developed primarily for IT environments and pose challenges for manufacturers, particularly for small- and mid-sized enterprises (S&ME) that comprise much of the defense supply chain. Further action is required to both affect the environment on the shop floor and strengthen countermeasures against cyber-attacks and cyber espionage. These actions include providing enhanced training to personnel on the shop floor to detect cyber breaches, and installing countermeasures that can detect, thwart, and report attempts to infiltrate production systems, particularly industrial control systems (ICS). Because of limited resources, S&MEs may require assistance from prime contractors and the Federal government, particularly the DoD, DHS, and NIST, to implement cybersecurity practices.

Today’s DIB is a fluid and dynamic system, where dual-use manufacturing capabilities allow some measure of industrial surge and mobilization from non-DoD suppliers, when needed. Based on its assessment of the current situation, the CFAM JWG recommends that DoD adopt the following vision statement to guide future actions in securing the U.S. industrial base, including and beyond the DIB, from cyber-attacks: “DoD and defense prime contractors are catalysts for creating a robust cyber-resilient U.S. industrial base connected through trustworthy manufacturing networks that responds rapidly to national security needs.” To implement this vision, the CFAM JWG proposes four broad recommendations for improving the manufacturing cybersecurity environment:

- Establish, and adequately fund, a new program for Manufacturing Cybersecurity Capabilities in the Industrial Base, with a Deputy Assistant Secretary of Defense (DASD)-level Champion to improve the visibility, policy integration and implementation of cybersecurity measures that address the special needs of manufacturing systems
- Establish a Public-Private Partnership for Security in American Manufacturing to create a cost-shared consortium for government and industry collaboration focused on the niche needs of cybersecurity in manufacturing.
- Incentivize Modernization for Cyber-Secure Manufacturing to modernize factory production systems to improve security while increasing productivity and enhancing quality.
- Give high priority to Research and Development (R&D) in Cybersecurity for Manufacturing to invest in technologies that can improve cybersecurity in critical defense manufacturing applications but lack a demand signal and a path to transition.



## CFAM Joint Working Group Membership

Sean Atkinson, GLOBALFOUNDRIES

Robert Badgett, Consultant

Vicki Barbur, MITRE

Dean Bartles, John Olson Advanced Manufacturing Center, University of New Hampshire

Dawn Beyer, Lockheed Martin Corporation

Brench Boden, Digital Manufacturing and Design Innovation Institute

Martha Charles-Vickers, Sandia National Laboratories

David Chesebrough, National Defense Industrial Association

Donald Davidson, Office of the Department of Defense Chief Information Officer

Michael Dunn, Analytic Services Inc.

Scott Frost, Analytic Services Inc.

Aman Gahoonia, Office of the Secretary of Defense, Defense Microelectronics Activity

***Marilyn Gaska, Lockheed Martin Corporation***

James Godwin, PricewaterhouseCoopers LLP

Robert Gold, Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Jason Gorey, Six O'Clock Ops

Dan Green, US Navy, Space and Naval Warfare Systems Command

Daryl Haegley, OASD Energy Installations & Environment

Greg Harris, Manufacturing Technology Office of the Secretary of Defense, Acquisition, Technology & Logistics, Manufacturing and Industrial Base Policy

David Huggins, Georgia Tech Research Institute

Larry John, Analytic Services Inc.

Greg Larsen, Institute for Defense Analyses

Brynne McCord, Engility Corporation

Thomas McCullough, Lockheed Martin Corporation

Thomas McDermott, Georgia Tech Research Institute

Michael McGrath, McGrath Analytics LLC

Sean Miles, Defense Intelligence Agency

Michele Moss, Contract support to Office of the Department of Defense Chief Information Officer

***Heather Moyer, Crossroads Consulting LLC***

Catherine Ortiz, Defined Business Solutions LLC

Chris Peters, The Lucrum Group

Robert Pickett, Department of Defense Office of the Joint Chief of Staff J4, Knowledge-Based Logistics Division

James Poplin, Defined Business Solutions LLC

Anitha Raj, ARAR Technology



Adele Ratcliff, Office of the Secretary of Defense, Acquisition, Technology & Logistics, Manufacturing and Industrial Base Policy

Melinda Reed, Office of the Deputy Assistant Secretary of Defense for Systems Engineering

Craig Rieger, Idaho National Laboratory

Sergio Salinas, Wichita State University

Frank Serna, Draper

Stephanie Shankles, Contract support to Office of the Department of Defense Chief Information Officer

Devu Shila, United Technologies Research Center

Tim Shinbara, The Association for Manufacturing Technology

Joseph Spruill, Lockheed Martin Corporation

***Sarah Stern, Boeing, Boeing Commercial Aircraft Network Cyber Security***

Haley Stevens, Digital Manufacturing and Design Innovation Institute

Keith Stouffer, National Institute of Standards and Technology

Rebecca Taylor, National Center for Manufacturing Sciences

COL Bill Trautmann, Department of Defense Office of the Joint Chief of Staff J4, Knowledge-Based Logistics Division

Janet Twomey, Wichita State University

Irv Varkonyi, Supply Chain Operations and Preparedness Education (SCOPE)

Andrew Watkins, Digital Manufacturing and Design Innovation Institute

Mary Williams, Manufacturing Techniques Inc. (MTEQ)

Fran Zenzen, QRC Technologies Inc.

**Bold indicates Team Leader**

Underline indicates Integration Team Member



## TABLE OF CONTENTS

FOREWORD .....	III
<b>EXECUTIVE SUMMARY .....</b>	<b>VII</b>
<b>CFAM JOINT WORKING GROUP MEMBERSHIP .....</b>	<b>IX</b>
<b>THE MANUFACTURING CYBERSECURITY CHALLENGE .....</b>	<b>1</b>
MANUFACTURING IS UNDER ATTACK .....	1
IMPORTANCE OF A SECURE, ADAPTABLE U.S. INDUSTRIAL BASE .....	3
NATIONAL SECURITY IMPLICATIONS .....	4
STAKEHOLDERS BEYOND DoD .....	5
<b>UNIQUE CONSIDERATIONS .....</b>	<b>5</b>
OPERATIONAL TECHNOLOGY ENVIRONMENT .....	5
SMALL & MEDIUM-SIZED ENTERPRISES (S&MEs) .....	7
S&ME SPOTLIGHT: MICRO CRAFT INC. ....	9
<b>ACTIONS TO IMPROVE MANUFACTURING CYBERSECURITY .....</b>	<b>10</b>
ADDRESSING THE CHALLENGE .....	10
VISION FOR U.S. MANUFACTURING CYBERSECURITY .....	12
RECOMMENDATIONS .....	12
SUMMARY .....	15
<b>APPENDIX A : NDIA CYBERSECURITY STUDIES .....</b>	<b>A-1</b>
THE NDIA CYBERSECURITY FOR ADVANCED MANUFACTURING JOINT WORKING GROUP .....	A-2
SUMMARY OF TEAMS' FINDINGS .....	A-2
<b>APPENDIX B : REPORT OF CFAM JWG TEAM ON MANUFACTURING ENVIRONMENT .....</b>	<b>B-1</b>
<b>THE MANUFACTURING CYBERSECURITY THREAT .....</b>	<b>B-1</b>
UNDERSTANDING THE DEFENSE MANUFACTURING ENVIRONMENT .....	B-1
OPERATIONAL TECHNOLOGY VERSUS INFORMATION TECHNOLOGY .....	B-3
THREATS, VULNERABILITIES, AND CONSEQUENCES .....	B-5
NATIONAL DEFENSE IMPLICATIONS .....	B-9
EDUCATION, TRAINING AND AWARENESS .....	B-9
SPECIFIC CONCERNS FOR SMALL AND MEDIUM SIZE MANUFACTURERS .....	B-11



<b>APPENDIX C : REPORT OF CFAM JWG TEAM ON POLICIES, PLANS, &amp; IMPACTS REGULATIONS, POLICIES, AND PRACTICES .....</b>	<b>C-1</b>
EXISTING POLICIES, REGULATIONS, AND STANDARDS .....	C-3
FUTURE STANDARDS DEVELOPMENT .....	C-10
CYBER INCIDENT REPORTING AND COMMUNICATION PROCESS .....	C-11
DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENTS .....	C-11
DHS CYBERSECURITY INFORMATION SHARING ACT OF 2015 .....	C-12
AREAS FOR FURTHER RESEARCH & DEVELOPMENT .....	C-12
FINDINGS AND RECOMMENDATIONS .....	C-13
<b>APPENDIX D : REPORT OF CFAM JWG TEAM ON TECHNOLOGY SOLUTIONS .....</b>	<b>D-1</b>
THREAT ANALYSIS .....	D-1
AVAILABLE SOLUTIONS .....	D-3
TECHNOLOGY SOLUTIONS RECOMMENDATIONS .....	D-8
<b>APPENDIX E : CYBERSECURITY FOR ADVANCED MANUFACTURING JOINT WORKING GROUP TERMS OF REFERENCE .....</b>	<b>E-1</b>
<b>APPENDIX F : DEFENSE MANUFACTURING ENVIRONMENT DIAGRAM NARRATIVE .....</b>	<b>F-1</b>
<b>APPENDIX G : THREAT USE CASES .....</b>	<b>G-1</b>
<b>APPENDIX H : SUBJECT MATTER EXPERTS INTERVIEWED .....</b>	<b>H-1</b>
<b>APPENDIX I : TERMS AND ACRONYMS .....</b>	<b>I-1</b>

## Table of Figures

Figure 1: Percent of 2016 Cyber-espionage Attacks, By Industry	1
Figure 2: Total U.S. Manufacturers, 251,901 Companies, By Size	3
Figure 3: NDIA Seminal Study on Manufacturing Cybersecurity	4
Figure 4: Operational Environment Characteristics	6
Figure 5: Solutions are Needed Specifically for the OT Environment	10
Figure 6: Findings to Recommendations Crosswalk	14
Figure 7: NDIA Cybersecurity for Advanced Manufacturing Studies	A-1
Figure 8: CFAM JWG Government Participation	A-1
Figure 9: CFAM JWG Teams and Work Scope	A-2
Figure 10: The Defense Manufacturing Environment	B-2
Figure 11: Threat to Defense Superiority	B-9
Figure 12: Small and Mid-Size Enterprises (S&MEs)	B-11
Figure 13: Policy Gap Between Acquisition and Manufacturing	C-3
Figure 14: Covered Defense Information (CDI) Source: Bob Metzger	C-6
Figure 15: Representative Manufacturing Case Studies for Attack Tree Analysis	D-1
Figure 16: Threats – Attack Vectors – Potential Impacts	D-2
Figure 17: Case Study Reference Architecture	D-3
Figure 18: Manufacturing Security Management Plan	D-6
Figure 19: Smart Manufacturing Technology Convergence	D-6
Figure 20: Emerging Enterprise Technologies	D-8
Figure 21: Summary of R&D Recommendations	D-8
Figure 22: Defense Manufacturing Environment: Production	F-1
Figure 23: Defense Manufacturing Environment: Sustainment	F-4
Figure 24: Generic HVAC Diagram	G-2
Figure 25: Nominal Simplified Additive Manufacturing Flow	G-4
Figure 26: Nominal Simplified Production Data Flow	G-6

(This page intentionally blank)

## THE MANUFACTURING CYBERSECURITY CHALLENGE

### Manufacturing is Under Attack

Cyber-attacks against U.S. manufacturers are increasing rapidly in number and severity. In 2016, the manufacturing sector attracted the highest percentage of cyber-espionage attacks (see Figure 1). Most manufacturing systems are not nearly as well protected as many business systems. This situation leaves the U.S. industrial base at great risk, imperiling the country's economic stability and military advantage.

Individual cyber-attacks on any manufacturing network can jeopardize product integrity, risk valuable intellectual property (IP), and threaten product or production reliability. Coordinated attacks can damage entire industries or stymie the production of material critical to building and sustaining our military's weapon systems.

The danger is exacerbated by a rapid global trend toward digital manufacturing and advanced interconnectivity throughout the supply chain. These developments have been fueled by the rapid emergence of the Internet of Things (IoT) and the growing value of the data that comprises a manufacturing network's digital thread. An ever-increasing arsenal of sophisticated cyber-attack tools is available to individuals, criminal organizations, and nation states, further elevating the risk.

Many authoritative journalistic and industry reports clearly indicate that manufacturing is a key cyber target for traditional and industrial espionage and extortion. According to IBM Security Services, in 2016 ransomware and digital extortion got a foothold in nearly every industry and region<sup>2</sup>. In one incident, a precast concrete and construction services company with contractual ties to the US Navy was targeted by an attacker who threatened to sell stolen data unless a ransom was paid<sup>3</sup>. "Unauthorized access has taken hold as the leading cause of incidents for our clients."<sup>4</sup> More than 60% of the manufacturing-related cyber incidents in the 2015 Verizon Data Breach Investigations Report were attributed to cyber-espionage, most by "competitors trying to obtain IP, whether that be

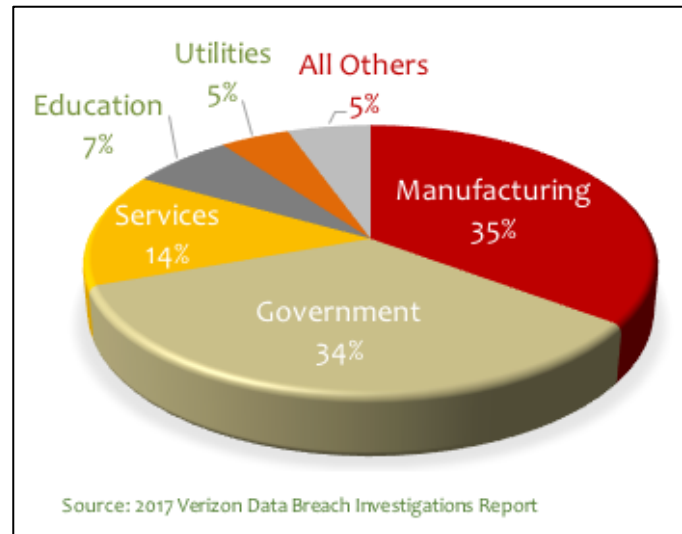


Figure 1: Percent of 2016 Cyber-espionage Attacks, By Industry

<sup>2</sup> IBM (2017). "Ransomware: How consumers and businesses value their data," IBM X-Force Research [https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-10908&S\\_PKG=ov55738&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US](https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-10908&S_PKG=ov55738&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US)

<sup>3</sup> <https://www.databreaches.net/thedarkoverlord-reveals-three-more-attacks-with-more-to-be-revealed/>

<sup>4</sup> IBM (2016). "A Survey of the Cyber Security landscape for manufacturing," IBM X-Force Research [no longer available online]

proprietary manufacturing processes, patents, designs or formulas.”<sup>5</sup> The FBI estimates that more than \$400 billion worth of IP leaves the U.S. each year.<sup>6</sup>

The 2017 Verizon Data Breach Investigations Report confirms earlier findings about the growing number of security breaches in the nation’s manufacturing infrastructure. Among the more troubling recent incidents was a 2016 attack that led to a distributed denial of service (DDoS) affecting hundreds of websites in the U.S.; in this instance, the Mirai malware employed IoT devices to carry out its attack. While the effects were relatively minor, the implications for industries reliant on industrial control systems (ICS) that are part of the IoT are most troubling.<sup>7</sup> Even more alarming was the recent campaign by the Petya ransomware (also known as WannaCry), which infected and denied access to both IT and OT systems worldwide. The later variant called notPetya, which initially appeared to be ransomware, was effectively wipeware capable of permanently destroying data and potentially causing physical damage to IT and OT systems.

DIB manufacturers are not exempt from such malicious cyber-tampering. The Department of Homeland Security (DHS) reported that between 2014 and 2016 the number of cyber-attacks against the nation’s critical manufacturing sector nearly doubled<sup>8</sup>, and the manufacturing sector attracts the greatest number of cyber-espionage attacks – the attacks that can diminish the U.S. military’s technical superiority through loss of intellectual property.

Most troubling for the manufacturing industry is a report issued in February 2016 by the Defense Intelligence Agency (DIA) that warned of the potential for Russian government hackers to penetrate U.S. ICS networks. Software being created by a Russian-based company is capable of exploiting vulnerabilities in supervisory control and data acquisition (SCADA) software used in nearly all manufacturing facilities and infrastructure systems. Officials have expressed concerns that hackers could gain control over the electrical grid, oil and gas networks, and water systems.<sup>9</sup> These same vulnerabilities can be exploited in manufacturing systems, which offer a much larger attack surface, contain much more valuable information, and present different constraints for potential solutions.

Today’s manufacturing environment poses unique cybersecurity challenges beyond the considerable technical complexities inherent in cyber-physical systems. These challenges stem from fundamental differences between information technology (IT) in the business enterprise and operational technology (OT) in the manufacturing environment. Too often, organizational stovepipes separate engineering, management and decision-making processes for enterprise business operations and the

---

5 Sikich (2016). “2016 Manufacturing Report: Taking your business to the next level and ensuring a successful future,” <http://www.sikich.com/insights-resources/thought-leadership/whitepapers/manufacturing-report-2016>, Sikich LLC.

6 <https://www.fbi.gov/video-repository/newss-the-company-man-protecting-americas-secrets/view>

7 Alex Bennett, “Top Cybersecurity Threats to Manufacturing in 2017.” *Manufacturing Business Technology*, 16 March 2017. <https://www.mbtmag.com/article/2017/03/top-cybersecurity-threats-manufacturing-2017>.

8 Cited in Jim Finkle, “U.S. Reports on Cyber-attacks on Manufacturing, Other Industries.” *Insurance Journal*, 15 January 2016. <http://www.insurancejournal.com/news/national/2016/01/15/395281.htm>

9 Bill Gertz, “DIA: Russian Software Could Threaten U.S. Industrial Control Systems.” *Washington Free Beacon*, 1 March 2016. <http://freebeacon.com/national-security/dia-russian-software-could-threaten-u-s-industrial-control-systems/>



production environment, a problem exacerbated by the inherently change- and risk-averse culture on the shop floor. Both the DoD and private industry face significant challenges in protecting the manufacturing process from nation-state cyber-attacks that target OT systems as the “soft underbelly” of the enterprise.

### Importance of a Secure, Adaptable U.S. Industrial Base

Since the outbreak of the Second World War, the U.S. has based both its warfighting and deterrence strategies on its powerful, innovative, flexible, and balanced industrial base. This innovative flexibility was tapped in unprecedented scale beginning in 1939, as manufacturing facilities designed to produce consumer goods quickly became, collectively, the “arsenal of democracy.” That adaptability enabled a shift back to a peacetime footing and sustained economic growth in the 1950s and 60s.

The U.S. economy is the largest in the world and manufacturing is a vital component of the nation’s economic engine. U.S. manufacturers continue to respond to the nation’s need for warfighting materials while concurrently producing goods for domestic and global commercial markets – markets that demand the same flexibility as the defense sector. With more than 250,000 manufacturers, the U.S. industrial base is dominated by small operations with fewer than 20 employees (see Figure 2).

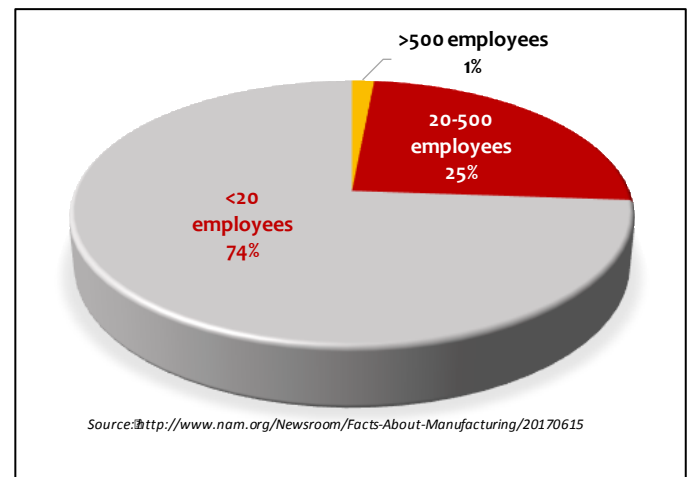


Figure 2: Total U.S. Manufacturers, 251,901 Companies, By Size

Today the path from design to production to distribution to employment of American-manufactured goods may begin in one part of the country (or the globe) and extend across the nation (or across continents). It is standard practice on large manufacturing tools (presses, drills, welders, automated assemblers—many of which are from overseas) for the original equipment provider to maintain an data link with the tool for diagnostic and upgrade purposes: “virtual globalization” can occur even when all physical processes are performed in the U.S. This access can provide an unintentional back door into the system.

The emerging digital manufacturing environment, often referred to as Industry 4.0, is a system built on automation, cyber-physical systems, cloud computing, and the Industrial Internet of Things (IIoT). New technologies allow manufacturers to produce reliable products efficiently and to adapt to changing requirements from both civilian and military customers. With this integration and flexibility, however, comes the potential for malicious actors to infiltrate key systems by gaining access to manufacturing networks. When successful, bad actors can extort ransom (in exchange for access to data or system control), copy sensitive proprietary information that can be sold to other companies or other governments, or install software that can affect a product’s performance. The potential consequences for national security cannot be ignored.

## National Security Implications

As Figure 3 illustrates, the 2014 NDIA White Paper, “Cybersecurity for Advanced Manufacturing” outlined threats to the DIB posed by malicious actors seeking to steal critical manufacturing information or to sabotage manufacturing systems by gaining access to the software used in OT, including the ICS used to assure product quality, reliability, and integrity. The White Paper also offered recommendations for a Cybersecurity for Advanced Manufacturing (CFAM) program to improve cybersecurity in the DIB. In 2016, NDIA organized a Joint Working Group to provide a blueprint for implementing the recommendations of the 2014 White Paper; their work is included as Appendices A through D.



Figure 3: NDIA Seminal Study on Manufacturing Cybersecurity

A partnership between the Federal government and the private sector is essential to address the serious implications for national defense posed by cyber breaches. Evidence already exists that state-sponsored efforts to infiltrate and steal information from companies involved in defense manufacturing have led to the development of military equipment remarkably like U.S. systems; it is no coincidence that several of the planes, drones, and vehicles deployed by China and Russia bear striking resemblances to ones in the U.S. inventory.

Equally troubling is the fact that adversaries who penetrate the security systems in processes used to produce arms and equipment for the U.S. military may have the capability to alter or halt production processes to affect these items’ reliability, safety, or security, putting the lives of service personnel at risk and materially degrading the ability of the nation’s fighting forces to succeed on the battlefield. Hence, developing and maintaining effective methods to secure the production process from conception to delivery of equipment to military units is essential. The U.S. industrial base, however, is comprised of tiers of contractors and suppliers possessing varying levels of cybersecurity sophistication. A large defense prime can share sensitive technical and program information with subcontractors in its supply chain, but if the subcontractors have weaker cyber protections, the information can be vulnerable to exfiltration or tampering. The Federal government can mandate regulations and specific protections for their prime contractors and, through contract flowdown requirements, can impose such requirements throughout the supply chain. While prime contractors should minimize the flowdown of information requiring protection, some flowdown to less-well prepared firms may be inevitable.

## Stakeholders Beyond DoD

As the foregoing discussion makes clear, cybersecurity is not a matter of concern for DoD alone. In fact, as Executive Order 13806<sup>10</sup> indicates, many government agencies have a stake in a secure manufacturing system: the Department of Homeland Security, Department of Energy, Department of Commerce, Department of the Interior, Department of Justice, Department of State, Department of Health and Human Services, Department of the Treasury, Department of Labor, Department of Transportation, Department of Agriculture, and the National Security Council. Many of these agencies are involved in overseeing or working with manufacturing firms; others are charged with securing the nation's economic infrastructure and providing defense against attacks by foreign governments and non-state actors. Hence, each can and should play a role in stopping cyber-crime, cyber-terrorism, and cyber-warfare to help build a manufacturing system in which vulnerabilities are minimized while operating efficiency is maintained.

Private sector manufacturing firms also have a stake in making their systems secure against infiltration and protecting the IIoT so they can increase the likelihood that their products and processes are reliable and secure from potential sabotage. Prime contractors engaged in or supporting defense manufacturing must have robust, active risk management and cybersecurity programs that consider their suppliers. They must also have well-founded confidence in their business partners' cybersecurity programs *before* enabling connections intended to support critical or sensitive communications. S&MEs also have a stake; both ensuring continued access to government and commercial contracts and protecting corporate IP make it imperative that firms implement measures to secure their OT and ICS from compromise. Hence, efforts of DoD to partner with the manufacturing industry to implement CFAM recommendations may serve as a model for other agencies to find ways to link with the private sector in promoting strong cybersecurity.

## UNIQUE CONSIDERATIONS

### Operational Technology Environment

The risk management process described in National Institute of Standards and Technology (NIST) Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, was written for Federal IT systems. Effective application to application OT systems requires a clear understanding of the differences between IT and OT. Compared to OT, IT systems and related business processes are more established and more focused on end-user support and efficiency. OT systems are developed outside the typical IT infrastructure, follow different standards, and have different priorities (e.g., safety, reliability, productivity) (see Figure 4). Unlike IT,

---

<sup>10</sup> White House Executive Order 13806, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," July 21, 2017.

the OT environment is not highly adaptable to change, which is often viewed as “disruptive,” especially for what are often custom-built production systems. In some cases, the potential benefit of a security update would not be considered worth the risk of disrupting operations and degrading productivity on the factory floor. Thus, change management is approached very differently in the OT environment.



Figure 4: Operational Environment Characteristics

The life span of an OT system hampers implementing accepted IT cybersecurity practices. Hardware in business systems might be updated every few years but the average life of U.S. industrial equipment is measured in decades. Given historical equipment lifecycles, especially in the DIB, many existing manufacturing systems will be in use for more than 15–20 years. Existing legacy systems were not designed with cybersecurity or the IIoT in mind; they are inherently unsecure, especially when networked. Frequently, legacy OT systems cannot handle the central processing unit (CPU) load for real-time processing; thus, concern about the impacts of latency on production impedes adoption of some cybersecurity solutions (e.g., active scanning and intrusion detection systems). Similarly, the OT environment is resistant to the use of software patches and updates that might interfere with legacy system operations.

In terms of corporate culture, communication and engineering gaps remain between IT and OT personnel because the two environments have traditionally been separated physically and organizationally. Nevertheless, as business realities drive the need for real-time data from many functions (including production) and the potential benefits of new technologies fuel the desire to connect production and non-production devices on the factory floor, the boundaries become blurred. Thus, communications and collaboration between IT and OT personnel must increase to identify and mitigate risks, especially where these systems connect.

Experts from the SANS Institute<sup>11</sup> declare that OT systems are “designed in unique ways and configurations that require the attacker to have extensive knowledge to impact them in a meaningful and designed way.” They also note that properly architected ICS contain “many layers of systems and detection sensors that an adversary must traverse” to access systems used in manufacturing. Connecting OT systems to the Internet, however, either directly or by proxy through another Internet-connected system, significantly undermines the inherent security advantages of a properly architected ICS. Additionally, the impacts of attacks on IT versus OT can differ greatly. While “denial of service to an IT system may be extremely significant to a business process,” manipulating sensors or processes

<sup>11</sup> Assante, Michael J, and Robert M. Lee (2015). “The Industrial Control System Cyber Kill Chain,” SANS Institute, available at <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297> p. 7.

in ICS “is more disturbing because it could lead to the failure of safety systems designed to protect human life or could induce the process to injure personnel.”<sup>12</sup>

The risk is heightened because production personnel are typically driven by the need to get new technology (e.g., sensors, mobile devices, 3D printers) installed and running, which can overshadow security considerations. Given this haste to deploy, IIoT will likely be adopted more quickly than it can be secured. The situation is analogous to when Wi-Fi emerged – it was installed everywhere, yet appropriate security protocols lagged by several years.

To overcome “human dimension” challenges, corporate leaders and cybersecurity professionals must understand and address valid shop floor concerns and priorities. Doing so will improve the likelihood the firm will successfully adopt both useful cyber hygiene practices and effective technology solutions in the near- and long-term.

For small businesses, this outcome is a potentially significant challenge; organic IT resources may be very limited, and OT personnel often do not consider their operations of interest to threat actors.

### Small & Medium-Sized Enterprises (S&MEs)

Small and medium-sized enterprises (S&MEs) present a special challenge for cybersecurity in manufacturing environments. S&MEs are critical to defense manufacturing because they produce most of the components that are integrated into our weapons systems; yet, these companies are often the most vulnerable to cyber-attacks. The 2017 Ponemon report on third-party data breaches, illustrates the challenge relevant to defense prime contractors: 56% of the respondents confirmed that they had experienced a data breach caused by a supplier and 42% reported that cyber-attacks against third parties resulted in misuse of their company’s sensitive or confidential information<sup>13</sup>.

Many S&MEs lack the technical staff to provide robust cybersecurity; and, unaware of the threat complexity, are unable to create a business case for investing in OT cybersecurity. An adversary seeking defense IP would likely target small component suppliers with lower cyber barriers than would be found at a single systems integrator. Having gained access to a small supplier, the attacker could find either the information they seek or the means (targets and data required to create a more effective spearfishing or watering hole attack) to gain access to the prime’s network.<sup>14</sup>

As the 2014 CFAM White Paper noted, efforts by S&ME could benefit greatly from DoD’s and their prime contractors’ technical and financial assistance. Enabling S&MEs to be key partners in cyber defense is critical to success. Today, as reported by Ponemon, 57% of the respondents are unable to determine if their vendors have adequate cyber-protections.

---

<sup>12</sup> Assante and Lee (2015), p. 11.

<sup>13</sup> Ponemon Institute LLC. (2017, September). *Data Risk in the Third-Party Ecosystem*. Retrieved October 4, 2017, from Opus Global Inc.: <https://www.opus.com/ponemon/>



Increasing cybersecurity protections at S&MEs and aligning IT and OT practices can convey specific advantages by minimizing costs for projects, procurement, licensing and overall support of the infrastructure. Nevertheless, creating such alignment requires an even more concerted effort to determine the extent and impacts of cybersecurity threats from a holistic, system-of-systems perspective. Thus, it is “essential that IT and OT security personnel, as well as national policy makers, fully engage the engineering community to uncover the scenarios that could be harmful at various facilities to help them understand the potential achievable goals of an adversary.”<sup>15</sup>

Neither the manufacturing industry nor DoD can unilaterally assure improvements in cybersecurity on the shop floor, elsewhere in the supply chain, or in the many peripheral activities that are key components of manufacturing. Therefore, to be effective, DoD or DoD-sponsored personnel should be deployed to partner with S&MEs to implement cybersecurity measures. DoD’s experience implementing Lean Six Sigma may be instructive: a factor in creating the environment for significant improvements was achieved through high-impact personal relationships, among other activities.

The implementation of DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, has enabled cooperation to begin. As stated in the memo, “Implementing DFARS USA002829-17-DPAP:” (emphasis added)

*The Department is working to assist the defense industrial base in executing its responsibility for ensuring that its supply chain, including small and mid-sized businesses, meets the requirements of the cybersecurity regulations. The Department routinely provides information and assistance to our defense industrial base partners at industry association meetings, joint government and industry meetings, small business training events, and quarterly meetings of the Defense Industrial Base Cybersecurity (DIB CS) Program.*

***To further facilitate communication with small businesses, the Department is leveraging the Procurement Technical Assistance Program (PTAP) to provide information addressing implementation of DFARS Clause 252.204-7012.*** Administered by the Defense Logistics Agency, the PTAP provides matching funds through cooperative agreements with state and local governments and non-profit organizations for the establishment of Procurement Technical Assistance Centers (PTACs). These centers, many of which are affiliated with Small Business Development Centers and other small business programs, form a nationwide network of counselors who are experienced in government contracting.

***The Department is also partnering with NIST Manufacturing Extension Partnership (MEP) to assist small and mid-sized U.S. manufacturers implement NIST SP 800-171.*** MEP is a nationwide system with centers located in every state. MEP centers are non-profit organization that partner with the Federal government to offer products and services that meet the specific needs of their local manufacturers.

The CFAM JWG applauds these efforts and recommends that the DoD–S&ME partnership be extended beyond DFARS compliance to additional activities that will enhance cybersecurity in S&MEs’ plants.

---

<sup>15</sup> Assante and Lee (2015), p. 12.

Specifically, DoD should conduct a joint effort with industry to:

- Improve the climate of cybersecurity awareness,
- Identify workable solutions to minimize risk,
- Implement solutions on the factory floor and throughout the supply chain to include machine tool providers as an integral part of the process, and
- Invest in people through direct DoD participation has a high potential to immediately improve S&ME cybersecurity.

#### **S&ME Spotlight: Micro Craft Inc.**

Current challenges faced by manufacturers, particularly S&MEs, are illustrated in the experience of Micro-Craft, a 57-employee firm focusing on design and production of components for the defense and aerospace industries.



While DFARS Clause 252.204-7012 does not require certification of the NIST SP 800-171, Micro Craft has been working aggressively to improve cybersecurity in their manufacturing systems. The company has revised business practices and implemented internal controls to safeguard data that falls under the categories “Covered Defense Information” and “Controlled Unclassified Information.” The company plans to meet DFARS Clause 252.204-7012 requirements by the December 31, 2017 deadline, and is implementing the requirements of NIST 800-171 in business processes and management systems.

Micro Craft participates in the DoD MANTECH Securing American Manufacturing effort. Micro Craft’s goal is to meet DoD requirements for secure OT systems. But the costs associated with assessment, implementation, and continuous monitoring impact their bottom line. Security infrastructure, hardware and software upgrades, and maintenance costs have increased overhead costs.

Of even greater concern for DoD, one of the OEMs with whom Micro Craft does business has informed the company that some suppliers will no longer support the OEM because it will be too costly to implement DFARS Clause 252.204-7012. However, to date only one OEM has contacted Micro Craft to inform the company of the requirement to implement mandated upgrades. Also, Micro Craft executives have found that the increased costs to improve cybersecurity put them at a competitive disadvantage.

Unless some effort is made to incentivize S&MEs to implement the NIST SP 800-171 requirements in DFARS Clause 252.204-7012 and, DoD may find that fewer companies will be able to comply with the terms and conditions of the contract making them ineligible to provide parts and components to prime contractors involved in defense manufacturing. These incentives must support the small and mid-size enterprises’ business model to ensure supply chain sustainability and viability.

## ACTIONS TO IMPROVE MANUFACTURING CYBERSECURITY

### Addressing the Challenge

The United States has already experienced the deleterious effects of worldwide hacking schemes in other sectors, and the 2017 Verizon report cited earlier indicates that attempts to penetrate OT and ICS in industry are increasing. Nevertheless, as Bryan Sartin, Verizon's Executive Director of Global Security Services, points out, while no system is impenetrable, "doing the [cybersecurity] basics well makes a difference."<sup>16</sup> In short, foundational action

- Training at all organizational levels
- Raising cybersecurity awareness with operators
- Incentives for improving cyber hygiene
- Implementing selected IT best practices
- Increasing interaction with IT network personnel and production engineers
- Including component security features in selection criteria



**Shop floor concerns and priorities need to be understood and addressed to improve solution adoption**

*Figure 5: Solutions are Needed Specifically for the OT Environment*

by industry and DoD is critical to thwarting efforts to compromise, cripple, or sabotage processes required to produce materiel for the nation's defense.

A threat as complex as cybersecurity for manufacturing calls for multiple, interconnected risk mitigation efforts. The overarching solution is to develop a strong CFAM program that can function effectively throughout the manufacturing ecosystem (see Figure 5). The CFAM JWG identified six activities to address the manufacturing cybersecurity challenge, discussed below. These activities establish the foundation upon which the subsequent recommendations were formed.

1. **Raise awareness** of the manufacturing cybersecurity threats to heighten management awareness and increase resources for solutions. Throughout the CFAM JWG research phase, raising awareness throughout manufacturing organizations was repeatedly listed as the single most powerful activity to improve manufacturing cybersecurity. Many manufacturers, especially S&MEs, are genuinely unaware of the threats to their OT networks and would likely address the threats if the danger of inaction was well understood.
2. **Provide training** at all organizational levels, from equipment operators to business owners, to immediately improve cyber hygiene and harvest lasting value from awareness campaigns. The CFAM JWG found that companies with security clearances from the Defense Security Services (DSS) had greater cyber protections in place than non-cleared companies because of DSS's Center for Development of Security Excellence. Additional training programs to include providing enhanced training to personnel on the shop floor so they can not only prevent but also detect cyber breaches could dramatically decrease network penetration detection time.
3. **Aggregate manufacturing cybersecurity activities** that exist, or are being created, across the Federal government to raise visibility, consolidate resources, and improve the pace of

<sup>16</sup> Quoted in Shaun Waterman, "Verizon's annual data breach report is depressing reading, again." Cyberscoop, 27 April 2017. <https://www.cyberscoop.com/verizon-annual-data-breach-investigations-report-depressing-dbir/>



progress. During the CFAM JWG study effort, pockets of manufacturing cybersecurity activities were found throughout DoD and the Federal government; many of these activities' managers were unaware of similar or adjacent efforts in other government offices. The national security imperative and S&ME dominance in the defense supply chain make DoD the logical lead to aggregate these activities under a single effort.

4. **Enable collaboration** among, and within, organizations working to better secure both OT and IT in manufacturers' operations. The CFAM JWG found multiple opportunities for collaboration to improve manufacturing cybersecurity, including among government offices; government and industry; IT and OT network technicians; design and production engineers; cybersecurity service providers and operations managers; and, manufacturing companies, their customers, and their equipment suppliers.
5. **Provide incentives** to manufacturers to upgrade facilities that will improve cybersecurity while enhancing productivity, and to equipment providers to improve security in their products. The CFAM JWG found a gap between cybersecurity offerings and shop floor priorities that must be understood to improve the creation and adoption of viable solutions. Factory equipment suppliers will likely be more inclined to improve their products' security features in partnership with customers that value those improvements during the purchase selection process.
6. **Develop technology** along two paths: immediately deployable improvements and long-term comprehensive solutions. Specifically, DoD could create or add to existing government-sponsored research programs designed to discover vulnerabilities within existing and emerging manufacturing networks. Examples include IARPA's CAUSE (Cyber-Attack Automated Unconventional Sensor); DARPA's VETS (Vetting Commodity IT software and firmware); DARPA's HACMS (High-Assurance Cyber Military Systems), a program designed to create technology to construct high-assurance cyber-physical systems; and DARPA's RADICS (Rapid attack detection, isolation and characterization), which can be employed in conjunction with the MITRE Corporation's ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), used to characterize and describe post-compromise adversary behavior in an enterprise network. Combining elements from these efforts into an overarching system to deliver an appropriate "plug-in" intermediary module could immediately increase cybersecurity while more comprehensive solutions are developed.

All the above initiatives must be pursued via a specific, measurable approach that collects the evidence required to ensure that the initiative is achieving the desired impact.

### Vision for U.S. Manufacturing Cybersecurity

The CFAM JWG recommends DoD adopt and implement the following vision statement, which is intended to guide future activities in support of manufacturing networks operating in a globally-connected environment:

**DoD and defense prime contractors are catalysts for creating a robust cyber-resilient U.S. industrial base connected through trustworthy manufacturing networks that respond rapidly to national security needs.**

Specific recommendations to implement this vision follow.

### Recommendations

Much progress has been made since the 2014 NDIA white paper, especially in the areas of procurement policies and contract requirements for protecting networks and controlled unclassified information. Nevertheless, DoD's implementation emphasis to date has been on enterprise IT systems and security practices, with only limited attention to OT, especially shop floor ICS systems and networks. There is recognition of the importance of ICS security outside DoD, but this is primarily in critical infrastructure settings rather than manufacturing systems. Cybersecurity for manufacturing is still an "orphan" in Federal cybersecurity policies and programs.

Absent recognition of implementation challenges and availability of DoD/OEM assistance for smaller manufacturers, the difficulty of compliance may drive some suppliers to exit the defense business. There is an opportunity for DoD leadership based on national security needs, with the potential for much broader impact across the entire U.S. industrial base. To seize this opportunity, we recommend that the USD(AT&L) successor organization:

1. Establish, and adequately fund, a new program for Manufacturing Cybersecurity Capabilities in the Industrial Base, with a DASD-level Champion and participation from DHS. The program's role is to advocate improved visibility and policy integration, as well as implementation of cybersecurity controls that address the special requirements of manufacturing systems as part of the overall DoD cybersecurity program. Specific near-term actions include:
  - a. Work with DoD stakeholders in cybersecurity policy, acquisition policy, sustainment policy, and procurement policy to ensure manufacturing requirements are adequately addressed in policy documents and implementation reviews; and develop separate guidance to protect OT networks where needed.
  - b. Work with the DoD Chief Information Officer (CIO), Defense Contract Management Agency (DCMA), Defense Security Service (DSS), Defense Logistics Agency (DLA) and industry to increase awareness of the importance and special requirements of manufacturing systems security. This task should be part of an overall cybersecurity campaign aimed at participants in supply chains, similar to other types of security and

- safety awareness campaigns, (for example, the cybersecurity awareness campaigns run by the Defense Security Service's Center for Development of Security Excellence).
- c. Sponsor programs in partnership with other government agencies (e.g. DHS, NIST, DOE, and others) and industry to advance training in "cyber hygiene" on the shop floor, bring about culture change at every level, and equip S&ME to become smart buyers of cybersecurity services and solutions.
  - d. Establish an Evidence-Based Manufacturing Cybersecurity program designed to 1) ensure that the various cybersecurity initiatives and campaigns have their intended effects, and 2) enable the compilation of data that can show which cybersecurity initiatives (technology, tactics, training, or procedures) have the best overall impact for a specified amount of resources.
2. Establish, and share the cost of, a Public-Private Partnership for Security in American Manufacturing. Use an innovative funding vehicle such as DoD's Other Transaction Authority (OTA, described in 10 U.S.C. § 2371 and § 2373) to establish a cost-shared consortium for government and industry collaboration focused on the niche needs of cybersecurity in manufacturing. Participants would include DoD and other interested Federal agencies, defense prime integrators, manufacturers in defense supply chains, commercial manufacturers, academia, standards organizations and solution providers (e.g. providers of ICS and sensors, technical data systems, IT/OT convergence services, and cybersecurity solutions and services). The partnership should:
- a. Develop and deliver workforce training in conjunction with OEM/prime contractor outreach to suppliers. The Defense Logistics Agency's (DLA) Procurement Technical Assistance Program (PTAP) could be leveraged to support this recommendation. (This effort may provide a delivery channel for recommendation 1.c above)
  - b. Serve as an Information Sharing and Analysis Center (ISAC) to gather information on cyber threats to manufacturing, solutions, and best practices, and to provide two-way sharing of information between the private and public sector, in coordination with other ISACs and the DIB Cybersecurity Program.
  - c. Coordinate industry use of manufacturing testbeds and cyber ranges for demonstrations and penetration testing. Build on the current Securing American Manufacturing program.
  - d. Develop a set of practices and implementation guides that apply the NIST Framework for Improving Critical Infrastructure Cybersecurity, aka Cybersecurity Framework, to meet the cybersecurity needs of industry members.
  - e. Perform additional functions defined in the process of structuring the partnership.

3. Incentivize Industrial Modernization for Cyber-Secure Manufacturing Through The Use of Innovative Contracting Authorities. Current ICS architectures, networks, processors, and sensors are much more secure than the legacy equipment in widespread use in most U.S. manufacturing operations. Industry experience shows that modernizing such systems can improve productivity and quality as well as security, yet most manufacturers are unable to justify the investment until current equipment reaches end of life. DoD could tip the balance on such investment decisions by, for example, subsidizing ICS vendors to offer discounts to manufacturers working on defense contracts. We recommend that:
  - a. DoD issue a Request for Information (RFI) inviting industry concepts for incentivizing ICS cyber modernization for defense suppliers, including a business case for the concept.
  - b. Based on favorable responses to the RFI, allocate resources to execute the program and obtain Congressional support for the initiative.
4. Give High Priority to R&D in Cybersecurity for Manufacturing through Targeted Project Funding. Ongoing DARPA work in this area is promising, as are emerging commercial technologies. Existing OSD and Service programs and the Small Business Innovative Research (SBIR) program have the latitude to invest in technologies that can improve cybersecurity in critical defense manufacturing applications, but need a demand signal and a path to transition. We recommend designation of this topic as a priority for S&T planners and offer the technology ideas in Appendix D as examples. Specific actions are for the USD(R&E) to:
  - a. Direct the appropriate Reliance<sup>21</sup> Communities of Interest to identify and coordinate increased S&T investments in cybersecurity for manufacturing systems.
  - b. Include cybersecurity topics in future SBIR announcements, and give fast track priority to any promising SBIR Phase I efforts that result.

	Raise awareness	Provide training	Aggregate activities	Enable collaboration	Create incentives	Develop technology
<b>DoD program</b>	X	X	X	X	X	X
<b>Public-private partnership</b>	X	X	X	X	X	X
<b>Modernize facilities</b>		X		X	X	X
<b>R&amp;D</b>			X		X	X

Figure 6: Findings to Recommendations Crosswalk

## Summary

Combining manufacturing innovation and secure technological superiority will enable the United States to remain the world's dominant military power. Advanced manufacturing technology drives national economic performance, making it a critical enabler in fielding advanced technology weapon systems. The benefits companies are gaining by adopting smart manufacturing technology are fueling a quick, permanent transition to the Fourth Industrial Revolution (Industry 4.0). This revolution, however, opens gaping holes in security systems, expands the attack surface, increases vulnerability of the manufacturing supply base, and creates serious threats to national security.

Implementing the Cybersecurity for Advanced Manufacturing Joint Working Group recommendations detailed in this report will deliver high value for the warfighters and taxpayers. Creating high-impact collaborations will strengthen the nation's technology value chain, benefitting not only DoD but also the prime contractors who supply much of the materiel required for the nation's fighting forces and the small businesses that offer valuable innovation and are a source of much of the nation's economic growth.

The nation will benefit significantly by investing proactively in building a more secure DoD manufacturing infrastructure, creating a smarter defense against malicious actors, and allowing the United States, and particularly the Defense Industrial Base, to stay ahead of the cyber-threat throughout the supply chain. NDIA looks forward to continuing to work with DoD to realize the vision of a robust cyber-resilient U.S. industrial base connected through trustworthy manufacturing networks that respond rapidly to national security needs.

## APPENDIX A : NDIA CYBERSECURITY STUDIES

In 2013 the National Defense Industrial Association (NDIA) launched a study to examine the vulnerabilities unique to the Department of Defense (DoD) contractors' manufacturing operations, as cybersecurity challenges to industrial control systems (ICS) emerged. The white paper issued by the study team in May 2014 has become essential for understanding the complexity faced by DoD manufacturers. The document included recommendations to the Undersecretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) to better secure the Defense Industrial Base's (DIB) manufacturing networks. With USD(AT&L)'s

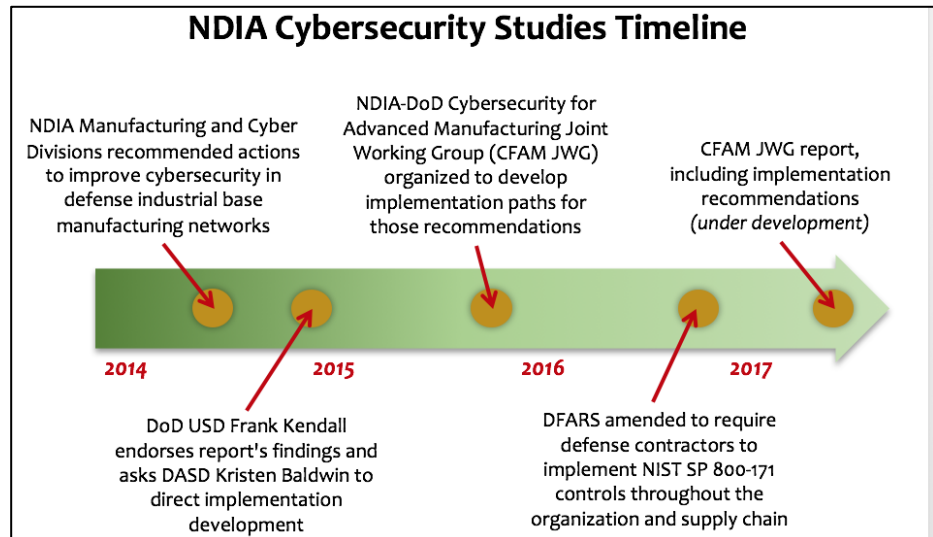


Figure 7: NDIA Cybersecurity for Advanced Manufacturing Studies

endorsement and support from the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)), a second study effort was launched in November 2015 as a government-industry joint working group tasked with developing implementation paths for the original study's recommendations.



Figure 8: CFAM JWG Government Participation

More than fifty members of the NDIA Cybersecurity for Advanced Manufacturing Joint Working Group (CFAM JWG) examined the defense manufacturing environment, the policy and regulatory landscape, and available and emerging technology solutions. The findings of these working groups are presented as Appendixes B, C, and D of this report. They represent work

accomplished over a 15-month period in a highly dynamic environment.<sup>17</sup> While some parts of this

<sup>17</sup> This Study complements the recently released National Center for Manufacturing Sciences White Paper *Balancing Productivity and Security: The New Cybersecurity Challenge for Manufacturers*, expanding the findings of that study and offering more detailed suggestions for cooperation between government and industry to improve cybersecurity in manufacturing.



paper undoubtedly will be outdated by publication, the implementation paths for the original study team's recommendations have been formulated to survive shifting conditions within the U.S. Government, manufacturing operations, and cybersecurity practices.

### The NDIA Cybersecurity for Advanced Manufacturing Joint Working Group

The NDIA CFAM JWG aligned NDIA divisions most germane to the manufacturing cybersecurity challenge (Cyber, Logistics, Manufacturing, and Systems Engineering) with their counterparts within the DoD. Team members included representatives of firms ranging from large companies to a woman-owned small defense manufacturer, academia, trade organizations, and federally funded research and development centers. Government participants included representatives from two branches of the

<b>Manufacturing Environment Team</b>  Team Leader: Marilyn Gaska, Lockheed Martin Corporation	Define the boundaries of the manufacturing environment for this study  Identify actions and activities that can have the greatest impact to improve cybersecurity in the manufacturing environment
<b>Policy Planning &amp; Impacts Team</b>  Team Leader: Sarah Stern, The Boeing Company	Review existing policies and regulations for applicability to CFAM  Determine additional administrative actions that could strengthen manufacturing cybersecurity  Assess breach reporting and communication processes for improvements
<b>Technology Solutions Team</b>  Team Leader: Heather Moyer, Crossroads Consulting LLC	Evaluate existing technical solutions available or under development to impact cybersecurity in the manufacturing environment  Recommend new technology development activities
<b>Integration Team</b>  Team Leader: Catherine Ortiz, Defined Business Solutions LLC	Create the CFAM JWG charter and scope Support other teams as needed Integrate teams' findings into final report

Figure 9: CFAM JWG Teams and Work Scope

Office of the Secretary of Defense (Office of the Chief Information Officer and Acquisition, Technology & Logistics), the Office of the Joint Chiefs of Staff, and the Department of Energy. Active involvement from such a large number of organizations demonstrates the high interest in, and deep commitment to, protecting manufacturing networks in the DIB. The CFAM JWG's diverse membership highlights this subject's critical dependencies across functional areas.

To develop implementation plans for the 2014 recommendations, the JWG was organized into four teams: Manufacturing Environment Team; Policy, Plans, and Impacts Team; Technology Solutions Team; and Integration Team. A list of Team Members is included at the beginning of the White Paper to which this report is attached as an Appendix. The NDIA CFAM JWG Terms of Reference, Appendix E, were created by the Integration Team to guide teams in their analyses and developing implementation paths for the 2014 recommendations. Each team selected a leader who set the method and tempo for team meetings. All four NDIA CFAM JWG teams began work by the end of February 2016.

### Summary of Teams' Findings

The Team on Manufacturing Environment examined relevant cybersecurity threats and vulnerabilities in the manufacturing environment and determined ways these can be mitigated; the Team also explored options for creating a methodology for measuring risks and monitoring threats and

vulnerabilities. An extensive review determined that currently there a notable gap exists between those involved in providing security for IT and those charged with securing OT, the integrated systems used in manufacturing. The Team determined that additional training of key personnel and increased focus on challenges faced by small and mid-sized manufacturers will be required to develop a culture of awareness and improve human performance and automated systems to strengthen the industry's capability to thwart the efforts of malicious actors intent on compromising OT systems. The Team's report is at Appendix B.

The Team on Policies, Plans, & Impacts identified relevant federal regulations, industry publications, mandated policies, and current practices that affect cybersecurity in the DIB. Their investigation revealed that numerous government agencies either mandate or provide guidance for cybersecurity, but that most documents focus on IT rather than OT. As a result, the Team Report (Appendix C) includes recommendations for modifying existing publications to provide specific directives or guidance applicable to manufacturing.

The Team on Technology Solutions looked at existing or planned technology solutions that might increase cybersecurity in manufacturing. To complete their task, the Team developed three case studies that focused on key components of cybersecurity: confidentiality, integrity, and availability. Their analysis revealed more than a dozen potential vulnerabilities in OT systems. Additionally, while the Team found that technology solutions are available to mitigate or eliminate some of these vulnerabilities, the need for changes in business practices is as important as the employment of technology if real improvements are to be made in securing components of manufacturing systems. The Team's report is at Appendix D.



## APPENDIX B : REPORT OF CFAM JWG TEAM ON MANUFACTURING ENVIRONMENT THE MANUFACTURING CYBERSECURITY THREAT

### Understanding the Defense Manufacturing Environment

The NDIA Cybersecurity for Advanced Manufacturing Joint Working Group (CFAM JWG) Manufacturing Environment Team (MET) was tasked to answer the following three questions about cybersecurity for advanced manufacturing in the Defense Industrial Base:

- What are the relevant cybersecurity threats, vulnerabilities, and consequences?
- How can cybersecurity risks in manufacturing environments be identified and mitigated?
- How do we create a methodology to continuously measure these risks and constantly monitor threat and vulnerability?

The overarching question is, “What can DoD and industry do to help manufacturers address threats and vulnerabilities, mitigate risks, and continuously assess the effectiveness of their efforts?”

The first step in addressing these questions was to develop a clear understanding of the context in which “DoD and industry ... [must] work together to manage risks [to the digital thread] at every level of the enterprise, including the factory floor.”<sup>18</sup>

The Defense Manufacturing Environment (DME) (Figure 10) shows the digital thread as digitally created, stored, and exchanged information that supports the manufacturing and sustainment processes of modern products. The digital thread exists throughout the product lifecycle. The DME includes major manufacturers and their networks of smaller suppliers, R&D labs, and OEMs that manufacture and support the industrial control systems (ICS) they use.

Nearly every organization is connected to the Internet and has perimeter cyber defense capabilities; generally, however, smaller suppliers have far less capability and cyber expertise than larger companies, making them far more inviting targets for cyber-attacks, especially once their affiliation with a larger supplier becomes public knowledge.<sup>19</sup> Cyber-attacks could affect one or more of the production functions shown at the bottom of the figure.

---

<sup>18</sup> NDIA (2014). *Cybersecurity for Advance Manufacturing: A White Paper*, National Defense Industrial Association Manufacturing and Cyber Divisions, Arlington, VA, p.1.

<sup>19</sup> See Appendix G for more details, including sample use cases involving attacks against the confidentiality, integrity and availability of elements of the DME.

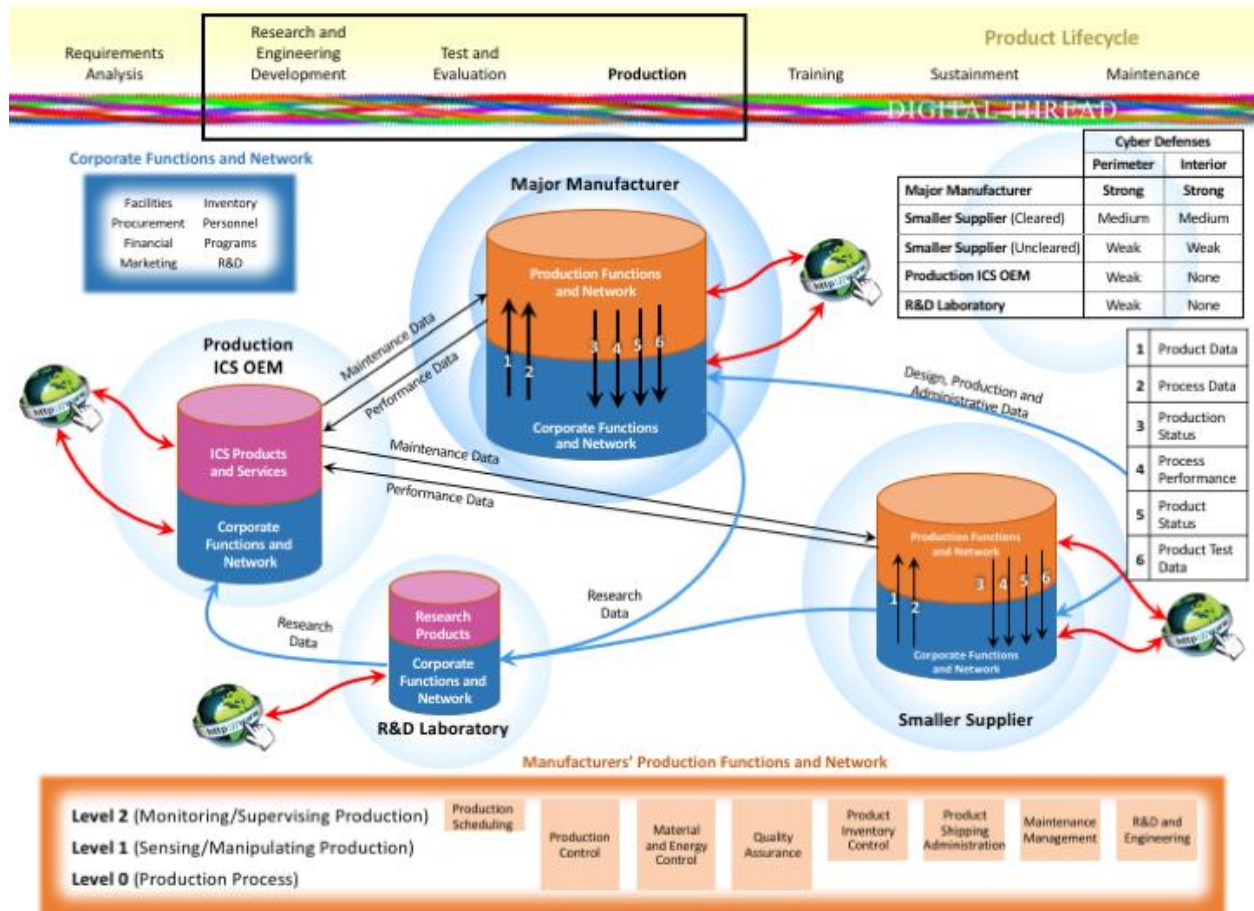


Figure 10: The Defense Manufacturing Environment

To represent the sustainment phase, a diagram like Figure 10 would also include the U.S. Government Sustainment System, which exchanges relevant data with smaller suppliers and major manufacturers. A vast set of potential attack opportunities present themselves in this even more distributed system of systems. It is critical to recognize that, in addition to vulnerabilities inherent in this portion of the life cycle, every product used to sustain or maintain fielded DoD capabilities was created by a DME like the one shown in Figure 9.

The DME diagrams and use cases (Appendix F) show that the digital thread is long and may present adversaries opportunities to steal or alter critical design, product, and product control data. As continuing research indicates,<sup>20</sup> this threat is magnified when one realizes that test machines used to validate products can be compromised just as easily as design and production machines. The discussion in the rest of this report is founded in this reality.

Research has also shown that cyber attackers, even those with state sponsorship, prefer to use easy, cheap penetration methods whenever possible. Hence, program managers, manufacturers, and other

<sup>20</sup> See, for example, the work of the Virginia Tech Applied Research Corporation referred to at <https://www.vt-arc.org/applied-r-d/>

suppliers can examine the digital thread to identify potential threats to individual suppliers and manufacturers. They can also highlight points at which risk management may be the weakest, because these will be places cyber attackers will try to exploit as part of what the SANS Institute ICS team describes as being not “one-off attacks,” but carefully planned, with “reconnaissance, multiple attacks and adjustments” that can occur “over the course of months.”<sup>21</sup>

### Operational Technology versus Information Technology

As reported in the NDIA 2014 CFAM White Paper, business and financial concerns are accelerating the drive to increase interconnectivity among manufacturing systems and connect them to enterprise business systems and information resources. It is, therefore, imperative that firms engaged in or supporting defense manufacturing develop robust, active risk management and information security programs. They must also have well-founded confidence in their business partners’ cybersecurity programs *before* enabling connections intended to support critical or sensitive communications. As the use cases in Appendix G show, this is especially true when the firm plans to digitally transmit or receive data related to product design, production, test, or maintenance.

Today’s manufacturing environment poses unique cybersecurity challenges beyond the considerable technical complexities of cyber-physical systems. These challenges stem from fundamental differences between IT and OT, organizational stovepipes that separate management and decision-making processes for enterprise business operations and the production environment, and the inherently change- and risk-averse culture on the shop floor.

IT systems and related business processes are more established and more focused on end-user support and efficiency. OT systems are developed outside the typical IT infrastructure, follow different standards, and have different priorities (e.g., safety, quality, productivity). IT systems run interruptible business processes and can be backed up frequently with relative ease; the nature of the risk in an OT environment is much more physical (loss of product, compromised quality, equipment or facility damage, human safety). The OT environment is not highly adaptable to change, which is viewed as “disruptive.” In some cases, the potential benefit of a security update would not be considered worth the risk of disrupting operations and degrading productivity. Thus, change management is approached very differently in each environment.

Another fundamental difference is the life span of an IT system versus an OT system. Hardware in business systems might be updated every few years because of technology advancements, but the average age of US industrial equipment is more than 10 years. Given historical equipment lifecycles, especially in the defense industrial base, many existing manufacturing systems will be in use for another 10-20 years. These legacy systems were not designed with cybersecurity or the Internet of Things (IoT) in mind and are inherently insecure, especially when networked.

---

<sup>21</sup> <http://ics.sans.org/media/control-systems-are-a-target-poster.pdf>

Frequently, unlike IT systems, OT legacy systems cannot handle the CPU load for real-time processing; thus, concern about latent impacts on production impedes adoption of some cybersecurity solutions (e.g., active scanning and intrusion detection systems). Similarly, the OT environment is resistant to the use of software patches and regular updates that might interfere with legacy system operations. On the shop floor, the cost of security is time (in the form of latency or down-time), which equates to inefficiency and risk; this drives cautious and conservative decision making.

In terms of corporate culture, a communication gap remains between IT and OT personnel because the two environments have traditionally been physically air gapped and organizationally separated. Today, as business realities drive the need for real-time data from many functions (including production) and new technologies fuel the desire to connect production and non-production devices on the factory floor, the boundaries are becoming blurred. As a result, communications and collaboration between IT and OT personnel must increase to identify and mitigate risks, especially where these systems connect. For small businesses, this is a potentially significant challenge; organic IT resources may be very limited, and OT personnel often do not consider their operations as being as interesting to threat actors as IT. The risk is heightened by the fact that production personnel are typically driven by the need to get new technology (e.g., sensors, mobile devices, 3D printers) implemented and running, which can overshadow security considerations. Given this haste to deploy, the IoT will likely be adopted faster than it can be secured, analogous to when Wi-Fi emerged – it was installed everywhere, yet appropriate security protocols lagged by several years.

---

*When applied correctly, the characteristics of OT systems convey immediate advantages from a cybersecurity perspective. But these advantages disappear when OT systems are directly or indirectly connected to the Internet.*

---

Unlike IT systems, OT systems are “shaped by the underlying engineering” and “designed in unique ways and configurations that require the attacker to have extensive knowledge to impact them in a meaningful and designed way. [I]n a properly architected ICS, there are many layers of systems and detection sensors that an adversary has to traverse ... to gain access to the ICS components.”<sup>22</sup> Connecting OT systems to the Internet, however, either directly or by proxy through another Internet-connected system, significantly undermines the inherent security advantages of a properly architected ICS. Moreover, not all manufacturers have the technical or financial wherewithal to create a properly architected system of systems on their own. Additionally, the impacts of attacks on IT versus OT can differ greatly. While “denial of service to an IT system may be extremely significant to a business process,” in ICS “the manipulation of sensors or the process is more disturbing because it could lead

---

<sup>22</sup> Assante and Lee (2015), p. 7.

to the failure of safety systems designed to protect human life or induce the process to injure personnel.”<sup>23</sup>

### Threats, Vulnerabilities, and Consequences

Many authoritative journalistic and industry reports clearly indicate that manufacturing is a key cyber target for traditional and industrial espionage and extortion. For example, as far back as April 2009, the *Wall Street Journal* reported that “[s]ix current and former officials familiar with the matter confirmed that the [F-35] program had been repeatedly broken into. The Air Force has launched an investigation.”<sup>24</sup> The implication is that technology stolen from the F-35 program was instrumental in creation of China’s J-31 fifth-generation stealth fighter.<sup>25</sup> More recently, IBM reports that their “average client company in the manufacturing industry [automotive, electronics, textile, and pharmaceutical companies] was found to have experienced just over 58 million security events – or 10 percent more [than reported in the 2015 report that covered a similar timeframe] ... Unauthorized access has taken hold as the leading cause of incidents for our clients.”<sup>26</sup> More than 60% of the manufacturing-related cyber incidents in the 2015 Verizon Data Breach Investigations Report were attributed to cyber espionage. “Most commonly, attacks are attributed to competitors trying to obtain intellectual property, whether that be proprietary manufacturing processes, patents, designs or formulas.”<sup>27</sup>

Sound risk management requires each organization to develop a rich picture of relevant threats and vulnerabilities. This picture includes understanding adversaries’ tactics, techniques, and procedures (TTPs). Manufacturing firms and their supplier networks must assess their vulnerability to each type of threat source and each relevant vulnerability category. The *NIST Risk Management Framework*<sup>28</sup> advocates a nine-step approach<sup>29</sup> to this task. Good risk management requires knowledge and experience from multiple disciplines.

Experience has shown that the use of shared language makes it far easier for firms and governments to understand and address common issues. Fortunately, publications such as NISTIR 7621, Revision 1,

---

<sup>23</sup> Assante and Lee (2015), p. 11.

<sup>24</sup> Gorman, S. A. Cole and Y. Dreazen (2009), “Computer Spies Breach Fighter-Jet Project,” *The Wall Street Journal*, accessed 4 Nov 2016 at <http://www.wsj.com/articles/SB124027491029837401>.

<sup>25</sup> Photo via Airliners.net by WC, from Weisgerber, M. (2015). “China’s Copycat Jet Raises Questions About F-35,” *Defense One*, September 23, 2015, accessed 7 Nov 2016 at <http://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/>.

<sup>26</sup> IBM (2016). “A Survey of the Cyber Security landscape for manufacturing,” IBM X-Force Research, accessed 4 Nov 2016 at <https://public.dhe.ibm.com/common/ssi/ecm/se/en/se912351usen/SE912351USEN.PDF>.

<sup>27</sup> Sikich (2016). “2016 Manufacturing Report: Taking your business to the next level and ensuring a successful future,” <http://www.sikich.com/insights-resources/thought-leadership/whitepapers/manufacturing-report-2016>, Sikich LLC.

<sup>28</sup> <http://csrc.nist.gov/groups/SMA/fisma/framework.html>

<sup>29</sup> <http://csrc.nist.gov/groups/SMA/fisma/documents/risk-management-framework-2009.pdf>, slide 3. The steps are: Categorize the system (including framing and assessing the risks), Select baseline controls, Refine controls based on the risk assessment, Document the controls in a system security plan, Implement the controls, Assess their effectiveness, Determine firm-level risk and tolerance, Authorize system operation informed by the assessment, and Monitor and adjust the effectiveness of controls over time.



*Small Business Information Security: The Fundamentals*,<sup>30</sup> the *NIST Cybersecurity Framework*,<sup>31</sup> and related Special Publications, including the emerging *NIST SP 800-181, NICE Cybersecurity Workforce Framework (NCWF)*,<sup>32</sup> offer useful lexicons that define key cybersecurity concepts and roles. *NIST Special Publication 800-82 revision 2*<sup>33</sup> is a particularly valuable resource for organizations seeking to understand cyber threats, vulnerabilities, and consequences to manufacturing.

NIST's recommended process for identifying and managing risk<sup>34</sup> begins with defining the threats to the organization within the context of the external environment. Applying the risk model requires identifying one or more threat sources and characterizing vulnerabilities. As Figure 4 shows, NIST SP 800-82r2<sup>35</sup> lists four types of threat sources (adversarial, accidental, structural and environmental) and six categories of vulnerabilities, along with sub-types and sub-categories (see Tables C-1 – C-7 in the NIST SP for details). Note that vulnerabilities can be mutually supporting.

Cyber attackers may strike for a variety of reasons under the umbrella of the “Confidentiality-Integrity-Availability” triad. Researchers rate the relative difficulty of conducting the types of ICS attacks,<sup>36</sup> which JWG members mapped to the CIA triad, from easiest to most difficult:

- Compromise ICS Security (Confidentiality)
- Exfiltrate Information (Confidentiality)
- Disrupt the ICS (Availability)
- Damage the ICS (Availability)
- Low Confidence Process Effect (Integrity)
- High Confidence Process and/or Equipment Effect (Integrity and Availability)
- Successful Attack with Re-Attack Option (Confidentiality, Availability, and Integrity)

---

<sup>30</sup> See <https://doi.org/10.6028/NIST.IR.7621r1>.

<sup>31</sup> <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

<sup>32</sup> <http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-181>

<sup>33</sup> <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

<sup>34</sup> NIST SP 800-30 r1, *Guide for Conducting Risk Assessments*, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.

<sup>35</sup> *Guide to Industrial Control Systems Security*, Revision 2, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>.

<sup>36</sup> Adapted from Assante and Lee (2015), “ICS Attack Difficulty Scale.”

- *Threat: “any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.”*
- *Threat Source: “The intent or method a threat may use to exploit] a vulnerability through either intentional or unintentional means”*
- *Vulnerability: “a weakness in an information system (including an ICS), system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.”*
- *Predisposing Conditions: “properties of the organization, mission/business process, architecture, or information systems that contribute to the likelihood of a threat event.”*
- *Threat Event: “an event or situation that has the potential for causing undesirable consequences or impact.”*
- *Incident: “When a threat event occurs it becomes an incident that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.”*

Assante and Lee make a critical point about the relative importance of confidentiality attacks. “In many cases, there is significantly more value ... in performing espionage than in perpetrating an actual attack that would include the destruction or manipulation of systems ... Therefore, it is important to identify and remediate adversary intelligence efforts – even if there is no immediate danger or business impact.”<sup>37</sup> Confidentiality attacks can enable adversaries to identify individuals for subsequent targeting, discover and devise ways to defeat specific military capabilities, and ascertain patterns of capability use that can be exploited when needed. All of these outcomes can threaten critical DoD capabilities at critical times.

Availability and integrity attacks can be either simple or complex: “a simple denial of service that disrupts the ICS is significantly easier to achieve than manipulating the process in a designed way or being able to attack the system and have the option of re-attacking [it].”<sup>38</sup> In general, attacks seeking to “achieve functional impact fall into three categories: loss, denial, and manipulation. They include a loss of view, denial of view, manipulation of view, denial of control, loss of control, manipulation of

<sup>37</sup> Assante, Michael J, and Robert M. Lee (2015). “The Industrial Control System Cyber Kill Chain,” SANS Institute, available at [https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain36297#\\_\\_utma=195150004.1133142235.1475771286.1475771286.1477498978.3&\\_\\_utmb=195150004.4.9.1477499205337&\\_\\_utmc=195150004&\\_\\_utmx=&\\_\\_utmz=195150004.1475771286.1.1.utmcsr=\(direct\)|utmccn=\(direct\)|utmcmd=\(none\)&\\_\\_utmv=&\\_\\_utmk=14654967](https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain36297#__utma=195150004.1133142235.1475771286.1475771286.1477498978.3&__utmb=195150004.4.9.1477499205337&__utmc=195150004&__utmx=&__utmz=195150004.1475771286.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)&__utmv=&__utmk=14654967). p. 6.

<sup>38</sup> Assante and Lee (2015), p. 10.

control, activation of safety, denial of safety, manipulation of safety and manipulation of sensors and instruments.”<sup>39</sup>

Fortunately, meaningful availability and integrity attacks typically require “a campaign of efforts that enables access and provides sufficient information to devise an effect ... Understanding where an adversary is in his or her campaign can enable defenders to make better-informed security and risk management decisions ... By understanding the inherent advantages of well-architected ICS networks and by understanding adversary attack campaigns against ICS, security personnel can see how defense is doable.”<sup>40</sup> Integrity attacks “capable of significant process or equipment impact require adversaries to become intimately aware of the process being automated and the engineering decisions and design of the ICS and safety system.”<sup>41</sup>

Campaigns require adversaries to first plan and execute one or more confidentiality attacks to conduct reconnaissance and imbed communications capabilities within the network, unless the targeted firm has ICS components that can be accessed directly or indirectly via the Internet. Adversaries must then study information collected by their reconnaissance probe to identify desired targets, gain access to targeted data and systems, and create tailored means to affect them. This complex series of events offers defenders more opportunities to detect attacks, mitigate losses, and even defeat attacks. For this reason, JWG members concluded that DoD suppliers must place prime emphasis on preventing, detecting, reacting to, mitigating, and recovering from confidentiality attacks. Small and mid-size manufacturers especially would benefit from DoD’s experience and help to create and execute effective manufacturing cybersecurity programs. In concept, DoD could provide this help in the form of training provided by:

- military or civilian personnel from either or both the Active Duty, Reserve, and Guard components;
- programs affiliated with other government entities and programs (National Initiative for Cyber Education (NICE), NIST Manufacturing Extension Partnership (MEP)); or
- commercial providers, with DoD subsidizing costs as needed, possibly under authorities granted to the Office of Economic Adjustment.

Breaking the kill chain and thwarting the objectives of attacks of all types requires well-planned and focused efforts that hinge upon a sound and continuous effort to identify and mitigate risks.

---

<sup>39</sup> Assante and Lee (2015), p. 11.

<sup>40</sup> Assante and Lee (2015), p. 1.

<sup>41</sup> Assante and Lee (2015), p. 1.



## National Defense Implications

Cyber-attacks on any manufacturing network can jeopardize product integrity, risk precious intellectual property, and threaten production operations. In the DIB, where our military's equipment is produced, cyber-attacks have national security implications. Evidence already exists that state-sponsored efforts to infiltrate and steal information from companies involved in defense manufacturing have led to the development of military

equipment remarkably similar to U.S. end items; it is no coincidence that several of the planes, drones, and vehicles deployed in by China and Russia bear striking resemblances to ones in the U.S. inventory.

Equally troubling is the fact that adversaries who penetrate the security systems in processes used to produce arms and equipment for the U.S. military may have the capability to alter production to affect these items' reliability, safety, or security, putting lives of service personnel at risk and materially degrading the ability of the nation's fighting forces to be successful on the battlefield. Hence, developing and maintaining effective methods to secure the production process from conception to delivery of equipment to military units is essential.

## Education, Training and Awareness

Decision makers must recognize these realities and must have the ability to understand and manage risk to manufacturing. Tight connections between IT and OT systems directly affect security needs and risk. Mechanisms on both sides of the IT/OT divide must adapt, requiring decision makers to address issues including, but not limited to:

- *Ownership and accountability.* When considering the pros and cons of connecting OT and IT systems, decision makers must ensure they understand and appropriately balance the priorities of knowledgeable individuals from the business, operations, security, and technology communities. **Simply put, IT and OT systems should only be connected when the readily achievable upside far outweighs the potential downside.**
- *Conflicting cultures.* Each community in an organization may have its own culture. In terms of cybersecurity, this culture has a direct impact on the perceived importance of each element of the CIA triad, and the five dimensions of Trustworthiness highlighted in the 2016 NIST



Figure 11: Threat to Defense Superiority

Credit to Brian Hughes, Director of the Office of the Secretary of Defense Director, Joint Acquisition Protection and Exploitation Cell

*Framework for Cyber-Physical Systems.*<sup>42</sup> Individuals who work directly with OT often prize Availability above the other triad elements and Reliability and Safety above the other Trustworthiness dimensions. ***Finding positive ways to overcome cultural resistance is key to the success of industrial cybersecurity efforts.***

- *Cooperation versus maintaining competitive advantage.* The digital thread inherently makes firms potentially vulnerable to their partners' weaknesses. In the same way that it is in DoD's interest to help its suppliers simultaneously become both more secure and more efficient, it is in each firm's interest to help its partners in the production chain do the same. The complexity of business relationships in the DoD and commercial marketplaces can often motivate against cooperation. Decision makers at smaller firms may need help coping with the reality that ***every decision about when and how much to help others has the potential for both good and bad strategic impacts.***

The JWG members agree that alignment of IT and OT can convey specific advantages in terms of minimizing costs regarding projects, procurement, licensing, and overall support of the infrastructure. However, creating such alignment requires an even more concerted effort to determine the extent and impacts of cybersecurity threats from a holistic, system-of-systems perspective. As a result, it is "essential that IT and OT security personnel, as well as national policy makers, fully engage the engineering community to uncover the scenarios that could be harmful at various facilities to help them understand the potential achievable goals of an adversary."<sup>43</sup> As the 2014 CFAM White Paper noted, efforts by small and mid-size manufacturers could greatly benefit from DoD's technical and financial assistance. Therefore, JWG members recommend that DoD create or add to existing DoD-sponsored academic research programs designed to discover vulnerabilities within existing and emerging manufacturing networks. These programs could be executed under the purview of an existing DoD-sponsored University Affiliated Research Center (UARC) like the Systems Engineering Research Center (SERC).

---

<sup>42</sup> Section B.4 of the CPS Framework addresses five interdependent dimensions of system trustworthiness: reliability, resilience, safety, security and privacy. See [https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS\\_PWG\\_Framework\\_for\\_Cyber\\_Physical\\_Systems\\_Release\\_1\\_oFinal.pdf](https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_oFinal.pdf)

<sup>43</sup> Assante and Lee (2015), p. 12.

## Specific Concerns for Small and Medium Size Manufacturers

As mentioned earlier, small and medium-sized manufacturers often do not have the staff, expertise, or financial wherewithal to develop effective cybersecurity measures on their own. These firms are often challenged to balance requirements of production with the need to provide appropriate security. The demand for efficient manufacturing frequently takes precedence over concerns about vulnerabilities caused by their interconnectedness via electronic means.

- Often lack cybersecurity knowledge and resources
- Most have no full time cybersecurity staff
- Believe they are not targets, so they focus on perimeter defense for IT network
- Many lack a business case for investing in OT cybersecurity



**S&MEs are Critical to Defense Manufacturing**

Cost is another significant challenge. Based on feedback from subject-matter experts, the annual cost of compliance with DFARS Clause 252.204-7012, Oct 2016, is anticipated to be in the millions of dollars for Tier 1 suppliers. It is unlikely that second- and third-tier suppliers will have the technical skills, knowledge, or funding to comply, though DFARS

Figure 12: Small and Mid-Size Enterprises (S&MEs)

Clause 252.204-7012 requires every prime flow down the clause to subcontractors only when performance will involve operationally critical support or covered defense information, which is in general for a certain percentage of business. Also, international suppliers must be made aware of these requirements, and primes must work with them to leverage their native cybersecurity policies and correlate them to DFARS requirements. If these firms do not comply, the prime contractor can work with DoD to resolve the concern through other mechanisms.

## Workforce Collaborations

Collaborative efforts to train and equip the workforce are essential for effective cybersecurity. The JWG believes the following initiatives can have significant impact:

- Better **integration of cybersecurity** into engineering, computer science, and management curricula to increase awareness and mutual understanding of cyber-physical challenges and solutions across relevant disciplines; better education will develop a skilled workforce capable of implementing smart manufacturing infrastructure.
- Frequent **training for certification, assessment, and qualification** of workforces to keep abreast of latest technologies, standards, and guidance for cybersecurity for advanced manufacturing.
- Renewed focus on science and engineering education to **cultivate a manufacturing workforce** that can manage highly technical systems and allow for greater automation, freeing employees to put their talents to work on R&D, redefining the meaning of a career in manufacturing.
- Creation of a **platform to enable workforce mobility** of documents, real-time data, collaboration, and workflows from their existing enterprise systems directly to front-line

workers, using smart glasses that do not require them to take their hands off their equipment or break from their task to consult a manual or computer terminal.

### *Human Factors*

While advances in technology may be of great assistance in thwarting efforts by adversaries to infiltrate the digital thread and affect production, the JWG believes the key to effective cybersecurity begins with a trained, committed, and capable workforce. Therefore, the JWG recommends the following actions to address the human factor in creating effective cybersecurity in the DIB:

- OUSD(AT&L) should support workforce training specifically focused around the advances and implications of the digital thread, deployment of systems connected to networks and to the Internet of Things (IoT), and appropriate ways to manage a sensitive and vulnerable environment.
- Workforce training in the use of advanced tools like Augmented Reality (AR) and Virtual Reality (VR) is critical, as deployment of these systems adds additional threats if appropriate precautions are not mandated as part of the ‘use’ pattern from the onset. These devices will increasingly become part of the digital thread as the move to the Virtual Factory floor takes place. Future training sessions should be focused on these matters, and may be facilitated by:
  - Support for Training Courses being offered by NNMI’s DMDII in conjunction with AREA (Augmented Reality for Enterprise Alliance) in the area of functional requirements for AR in manufacturing.
  - Development of a Guidance Document to support the concept of Virtual Manufacturing as an outcome of the digital thread to get ahead of the curve for use of simulation, AR, and VR to allow the design, development, and fabrication of new products. DMDII has recently released the first version of its Digital Commons, so this vehicle can provide a good beta test case and can be adapted before widespread release into the industry.

## APPENDIX C : REPORT OF CFAM JWG TEAM ON POLICIES, PLANS, & IMPACTS REGULATIONS, POLICIES, AND PRACTICES

The CFAM JWG Team on Policies, Plans, & Impacts (PPI) was tasked to identify and review federal regulations, industry publications, mandated policies, and current practices that affect the practice of cybersecurity in the DIB. The Team's objectives were to provide recommendations on:

- Where and how to augment existing policies, regulations, and standards; and
- Best practices for breach reporting and communication.

The JWG Team found multiple government offices that issue cybersecurity policy, guidance, regulation or mandates, including the Department of Commerce's National Institute of Standards and Technology (NIST); the Department of Energy; the Department of Homeland Security; and several DoD organizations: The Office of the Undersecretary of Defense, Acquisition, Technology & Logistics (AT&L), the Missile Defense Agency, and the DoD Chief Information Office. However, most existing cybersecurity policy and guidance focuses on protecting IT rather than OT. When OT is included in the requirement, the guidance can be overwhelming for the small and medium enterprises (S&ME) that manufacture most of the components and parts used by DoD.

For their analysis, the PPI Team reviewed:

- Applicability of existing policies, regulations, and standards
- Gaps in policies, regulations, and standards
- Results of a survey of manufacturing OT network breach reporting and communication processes
- Constraints on industry and the government
- Breakdown of current activities on the protection of manufacturing networks

In completing their work the Team received support from the American Society of Mechanical Engineers (ASME), the Industrial Control Systems–Cyber Emergency Response Team (ICS-CERT), Jacobs Technology Group, the Office of DoD CIO (Defense Industrial Base Cybersecurity), the Office of the Undersecretary of Defense (Procurement and Acquisition Policy), and Rogers Joseph O'Donnell, PC.

The bulk of the PPI Team's research centered on existing policies, regulations, and standards surrounding cybersecurity on the manufacturing floor. To include all possible initiatives and guidance documents, the PPI Team reached both across and beyond DoD to include:

- Office of the Secretary of Defense (OSD)
  - Acquisition, Technology & Logistics (AT&L)
    - Systems Engineering (SE)
    - Logistics & Material Readiness (L&MR)
    - Defense Procurement Acquisition Policy (DPAP)
    - Defense Contract Management Agency (DCMA)
  - DoD Chief Information Officer (CIO)
  - Missile Defense Agency
- Department of Commerce (DOC)
  - National Institute for Standards and Technology (NIST)
  - National Cybersecurity Center of Excellence (NCCoE)
  - Hollings Manufacturing Extension Partnership (MEP)
- Department of Energy (DOE)
  - Idaho National Laboratory
- Department of Homeland Security (DHS)
  - National Protection & Programs Directorate (NPPD)
    - Cybersecurity and Integration Center (NCCIC)
      - Industrial Control Systems – Cyber Emergency Response Team (ICS-CERT)
  - Office of Infrastructure Protection (OIP)
    - Critical Manufacturing Sector (CMS)



## Existing policies, regulations, and standards

While emerging cybersecurity mandates and guidance documents show promise for increasing the DIB's data protection, the Team found a lack of applicable policies or regulations that directly address security of networks and devices on the factory floor. NIST's Special Publication 800-82 (SP 800-82), *Guide to Industrial Control Systems (ICS) Security*, provides guidance on how to secure industrial control systems; however, its length (247 pages) can be overwhelming for S&MEs that manufacture most of the parts and components used in military hardware and systems.

Unlike IT cybersecurity processes or protections developed for information and communications technology (ICT), electronic systems used in manufacturing operate in a unique environment. The factory floor is not just another server room; its ICS network is critical infrastructure, as it drives devices ranging from those controlling energy systems to ones manufacturing the nation's most sensitive defense systems.

Current law, policy, regulations, and guidance that may be modified to include protections for the factory OT environment includes:

- DoDI 5000.02, *Defense Acquisition System*
  - Program Protection Planning
- DFARS Regulations
  - DFARS Provision Section 252.204-7008, *Compliance with Safeguarding Covered Defense Information*
  - DFARS Clause 252.204-7009, *Limitation on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information*
  - DFARS Clause Section 252.239-7010, *Cloud Computing Services*
  - DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*
- NDAA FY2016 Section 1647, *EVALUATION OF CYBER VULNERABILITIES OF MAJOR WEAPON SYSTEMS OF THE DEPARTMENT OF DEFENSE*

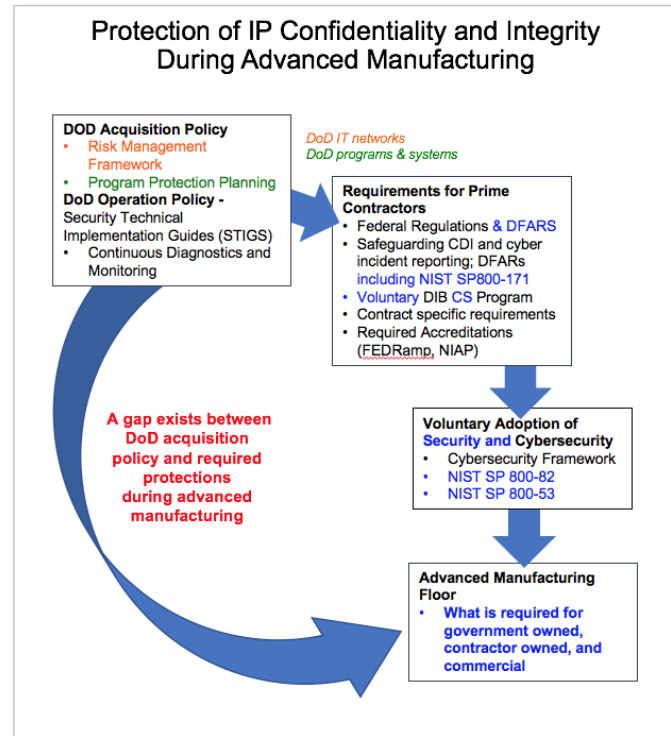


Figure 13: Policy Gap Between Acquisition and Manufacturing



- NIST Special Publication Guidance
  - NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*
  - NIST SP 800-171, *Protecting Controlled Unclassified. Information in Nonfederal Information*
  - NIST SP 800-82, *Guide to Industrial Control System (ICS) Security*
  - NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*
  - NIST Framework for Improving Critical Infrastructure Cybersecurity
  - NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*
  - NIST IR 8099, *Methods and Tools for Performance Assurance of Smart Manufacturing Systems*
  - NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*

The National Institute of Standards and Technology identifies the management of organizational risk as a key element in the organization's information security program. Developing an effective framework for selecting appropriate security controls is essential in protecting an organization's assets against cyber-attacks. "The Risk Management Framework [RMF] provides a process that integrates security and risk management activities into the system development life cycle."<sup>44</sup> Developing an effective RMF involves six essential steps:

- Categorizing a system and the information processed, stored, and transmitted by the system;
- Selecting a set of baseline security controls, and tailoring the baseline as conditions change;
- Implementing security controls and documenting how they are deployed within the system and in the environment in which the system is operated;
- Assessing security controls to determine that they are being implemented correctly, operating as intended, and producing desired outcomes;
- Authorizing operations of a system based on a determination of the risks posed to operations and assets, individuals, and other organizations affected by the system; key to this step is the determination that the risk is acceptable; and
- Monitoring security controls on an ongoing basis; this procedure includes assessing the effectiveness of security controls, documenting changes to the system or the environment

---

<sup>44</sup> The quote and outline that follow are adapted from <http://csrc.nist.gov/groups/SMA/fisma/framework.html>.

in which the system operates, conducting periodic security impact analyses, and reporting the state of the system's security to appropriate organizational officials.

Guidance on applying an effective Risk Management Framework to Federal Information Systems, NIST Special Publication 800-37 Revision 1. The following publications are key elements for implementation: FIPS 199; NIST Special Publication 800-53 Revision 4; and NIST Special Publication 800-53A Revision 4.

*DoDI 5000.02, Enclosure 14 and Program Protection Planning (PPP)*

In the defense acquisition world “the purpose of program protection is to give PMs an effective way to understand, assess, and prioritize the broad spectrum of security threats and attacks to the acquisition program, and to identify the right, cost-effective mixture of measures to protect against such attacks.”<sup>45</sup> Recommendation 3 in NDIA’s 2014 CFAM White Paper urged DoD to update PPP guidance to enhance protection of the digital thread. In January 2017, DoD updated their acquisition policy, DoDI 5000.02 to include assign and prescribe acquisition responsibilities for cybersecurity in the Defense Acquisition System.

DoD’s *Program Protection Plan Outline & Guidance* document has not yet been updated to explicitly align with the updated acquisition policy to require assessment of data used by, stored in, or transiting OT systems for protection as covered defense information as defined in the DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Furthermore, DoD has not explicitly included as Critical Functions those manufacturing functions that produce Critical Components. To this end, the JWG recommends modifying the “Expectations” paragraph under paragraph 3.1 (and other locations as needed) to add manufacturing specialists as key participants in the covered defense information, which includes controlled technical information, identification process. Corresponding changes should also be made to DoD’s *Program Protection Plan Evaluation Criteria* document, Chapter 13 of the *Defense Acquisition Guidebook*, as well as *Engineering for System Assurance* published by NDIA in cooperation with DoD.

---

<sup>45</sup> See [http://www.acq.osd.mil/se/initiatives/init\\_pp-sse.html](http://www.acq.osd.mil/se/initiatives/init_pp-sse.html).

## Defense Federal Acquisition Regulation Supplement (DFARS)

Manufacturers may understand the need to protect certain controlled technical information even if it is not classified, but they need specific guidance so they may be assured that their System Security plans for unclassified networks meet DoD expectations. DFARS Provision 252.204-7008 and Clause 252.204-7012 were developed to protect “Covered Defense Information” (CDI) against compromise, with separate focuses on compliance and safeguarding, respectively.

These regulations may prove of greatest value in assisting companies to identify information that must be protected and develop systems for doing so. Currently companies are experiencing problems using NIST SP 800-171 for guidance, as this document is geared toward IT, not OT; the documents were not written to address the needs of manufacturing.

DFARS rule 2013-Do18 did not add any unique or additional requirement for the Government to monitor contractor implementation of the required security requirements.

Contractor compliance with these requirements would be subject to any existing generally applicable contractor compliance monitoring mechanisms. Developing appropriate guidance is critical, however, as companies may be penalized if they cannot present evidence that they have implemented plans to secure covered defense information. In the future, as part of its surveillance activities, DCMA personnel will engage with contractors to implement the following actions in regards to cybersecurity: verify that the contractor has a system security plan; verify contractor submitted to DoD CIO within 30 days of any contract award made through Oct 2017, a list/notification of the security requirements not yet implemented; and verify contractor possesses DoD approved External Certificate Authority (ECA) issued medium assurance public key infrastructure (PKI) certificate to safeguard covered defense information that resides on or is transiting through a contractors internal information system or network. (IT and OT networks for covered defense information, including manufacturing). At present, many defense contractors do not believe ICS are covered by this rule. Better education is needed on “covered defense information” so that contractors understand both the need for appropriate handling and storage and the appropriate measures needed to provide adequate security for safeguarding covered defense information.

DFARS Clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting” also calls for contractors to protect technical information that, although unclassified, could be of use to those wishing to harm U.S. defense interests; it also requires that cyber incidents be reported to authorities. Companies must provide “adequate” security measures that will safeguard unclassified

“Covered defense information” means unclassified **controlled technical information** or other information, as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/categorylist.html>, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

- (1) Marked **or otherwise** identified in the contract, task order, or delivery order and **provided** to the contractor by or on behalf of DoD in support of the performance of the contract; or
- (2) Collected, **developed**, received, transmitted, **used**, or stored by or on behalf of the contractor **in support of** the performance of the contract.

Figure 14: Covered Defense Information (CDI)  
Source: Bob Metzger

controlled technical information *resident on or transiting* their unclassified information systems from unauthorized access and disclosure; this “covered defense information” must be labeled in accordance with Department of Defense Instruction 5230.24. Unfortunately, this requirement for safeguarding and reporting presume that the contractor has already implemented security controls in accordance with NIST SP 800-171. Furthermore, while the NIST SP 800-171 describes the kind of information that might be routinely considered OT, its repeated references to “information systems” may suggest that systems used on the factory floor are not subject to this requirement.

#### *NDA FY 2016 Section 1647, EVALUATION OF CYBER VULNERABILITIES OF MAJOR WEAPON SYSTEMS OF THE DEPARTMENT OF DEFENSE*

Congressional language in the FY2016 NDA Section 1647 focuses on protecting the mission or the weapons system rather than on the equipment that creates the weapons; however, an opportunity exists to include the manufacturing environment during the process of converting the Congressional language into defense regulations.

#### *National Institute of Standards and Technology (NIST)*

As NIST explains on its website, standardization activities in the United States are broad, complex, and decentralized. Hundreds of private organizations and public sector professionals participate in the work on such activities with funding provided by themselves or their employers, not by U.S. Government subsidy. Agreement on standards is reached by consensus; no single organization controls this industry-led process, even when government representatives participate. Some standards in technological areas which are subject to rapid change may be developed by industry consortia. Typically, participants in the standards development process include professional societies, trade associations, testing and certifying organizations, industry consortia, and organizations that only develop standards.<sup>46</sup>

---

<sup>46</sup> This paragraph is adapted from the NIST web site, <http://gsi.nist.gov/global/index.cfm/L1-5/L2-44/A-165>.

One example of the difficulty in creating a standard may be seen in the airplane manufacturing environment. The recent success of Boeing's KC-46A tanker program is a hybrid environment of commercial and defense. As stated in AINonline.com, "Boeing's strategy of using existing commercial procurement, inventory management and manufacturing processes to build the 767-2C, which will be 'provisioned' for the military tanker during fabrication and assembly on the commercial 767 line in Everett, Wash. Mission systems will be installed at a separate facility, a process modeled after Boeing's 'in-line' production of the P-8 Poseidon maritime patrol aircraft, a 737 derivative, for the U.S. and Indian navies." This poses an issue for levying cybersecurity standards in this type of environment. A DFARS cybersecurity manufacturing contract requirement would be levied in the defense manufacturing environment, but not necessarily in the commercial environment. Different regulations and standards are required for each environment.

Understanding the nature of the standards development process is a crucial first step in generating changes that can produce industry-wide standards for OT that are feasible, widely accepted, and truly useful in safeguarding ICS. While NIST provides a range of publications that include standards on cybersecurity for industry, little guidance in these publications is directly applicable to, or easily adaptable on, the factory floor. The following NIST publications may be useful, if adapted for manufacturing, to assist companies of all sizes in meeting the need to secure ICS.

*NIST SP 800-171 published June 2015; Revision 1 published December 2016*

NIST created Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, specifically to protect Controlled Unclassified Information (CUI) information systems and organizations operated outside the federal government. NIST SP 800-171 identifies 109 security safeguards in 14 families. These safeguards were developed to protect all forms of CUI, including the four types of covered defense information that are subjects of cybersecurity regulations implemented by DoD Safeguarding Covered Defense Information and Cyber Incident Reporting and Cloud Computing Defense Federal Acquisition Regulation Supplements. In December 2016, NIST released a Revision 1 to SP 800-171, increasing the controls to 110, that emphasizes "Nonfederal organizations to describe in a system security plan, how the specified security requirements are met or how organizations plan to meet the requirements. The plan describes the system boundary; the operational environment; how the security requirements are implemented; and the relationships with or connections to other systems. Nonfederal organizations should develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format". This revision merits

recognition by government contractors and by federal agencies planning to use their acquisition tools to improve the protection of CUI when provided to or furnished by their contractors.

*NIST SP 800-82, published May 2015*

NIST SP 800-82, *Guide to Industrial Control Systems Security*, provides guidance on securing Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. Drafted in 2006 and revised in 2013 and again in 2015, the document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate associated risks. The publication provides a high-level overview of the risk management process and identifies ICS-specific recommendations and guidance for each of the four major components (framing, assessing, responding, and monitoring). Furthermore, the document addresses special considerations for doing an ICS risk assessment, including appraisals of the impact that implementing cybersecurity measures has on safety and the physical environment.

Relying on guidance in NIST 800-53, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, NIST SP 800-82 includes an ICS overlay that provides tailored security control baselines for low, moderate, and high-impact ICS, adding supplementary guidance specific to ICS. While the overlay is intended to apply to all ICS systems in all industrial areas, it can be tailored to a particular sector such as manufacturing.

*NIST Framework for Improving Critical Infrastructure Cybersecurity also known as Cybersecurity Framework, published February 2014*

The NIST Cybersecurity Framework was developed in response to Executive Order 13636 (Improving Critical Infrastructure Cybersecurity). The 2014 release of the NIST Cybersecurity Framework provides some standards for protecting defense manufacturing. The Framework is based on a five-step process: Identify, Protect, Detect, Respond and Recover. The main categories covered by the Framework include Asset Management, Access Control, and Detection Processes. However, the Framework is focused on Information Technology, not oriented toward factory networks.

The Framework promotes protection of critical infrastructure by establishing standards, providing guidelines for implementation, and promoting best practices. Yet a 2016 survey conducted by Tenable Network Security of IT and security professionals across a range of industries revealed that only 30% of companies have adopted the voluntary framework.<sup>47</sup> While predictions are that the percentage will increase, the manufacturing sector continues to face problems in adapting IT-focused programs to its operations. While the DoD, under DFARS Clause 252.204-7012, requires implementation of NIST SP 800-171 to safeguard covered defense information, there have been requiring activities who have

---

<sup>47</sup> Roy Urico, "Few Adopt NIST Cybersecurity Framework." *Credit Union Times*, 29 March 2016. <http://www.cutimes.com/2016/03/29/few-adopt-nist-cybersecurity-framework-survey>.



written the requirement for implementing the Framework into some of its manufacturing contracts. The Framework is mainly IT based guidance; however, some of the integrated controls are from ISA/IEC 62443 (Industrial Automation and Control Systems).

#### *NIST IR 8099, published December 2015*

Released in December 2015, NIST IR 8099, *Methods and Tools for Performance Assurance of Smart Manufacturing Systems*, offers the manufacturing industry detailed information on assessing the performance of smart manufacturing systems. These systems, which introduce new technologies to enhance information flow within manufacturing systems and their ICS, have the potential to improve significantly the agility, productivity, and resilience in the production process. To collect data required to realize these improvements, control systems collect, analyze, and transmit data to decision makers and to equipment on the factory floor. Although NIST IR 8099 offers exceptionally detailed descriptions of methods to establish and maintain system performance using new technologies, the document offers little in the way of direct guidance for securing OT used in these new systems from cyber-attacks. Modifying the publication to include information on cybersecurity would give businesses looking to employ smart manufacturing systems a blueprint for assuring that their manufacturing operations could be protected from malicious actors intent on stealing sensitive information or altering production processes.

#### **Future Standards Development**

Efforts are underway by the Department of Homeland Security (DHS) to develop standards specifically applicable to the Internet of Things (IoT). In November 2016 DHS published a set of principles for securing IoT.<sup>48</sup> These include guidance developed by DHS emphasizing and encouraging the need to incorporate security at the design phase; promoting advanced security updates and managing vulnerability; building on proven security practices; prioritizing measures according to potential impact; promoting transparency across the IoT; and connecting production machinery and control systems carefully and deliberately. Such broad, common-sense guidance is not likely to influence manufacturers to change operations radically, as there is no legal requirement to implement even these broad recommendations.

Clearly there is a gap between the broad guidance currently available and methods of implementing specific measures for providing a secure environment on the factory floor. The most expeditious method of closing this gap would be to adapt standards currently in use for IT to meet the needs of manufacturers. A combination of requirements for implementing new security measures and best practices, coupled with incentives for meeting testable and measureable requirements, would be the best way to assure cooperation from manufacturers and improve security in the ever-changing environment on the factory floor.

---

<sup>48</sup> Charles Martin, "U.S. Issues Guidelines for IoT Security." *IoT Daily*, 18 November 2016. <https://www.mediapost.com/publications/article/289288/us-issues-guidelines-for-iot-security.html>.



## Cyber Incident Reporting and Communication Process

The status of manufacturing cyber incident breach reporting is best described as unsettled. Although manufacturers have access to tools and resources for breach reporting through DHS, the uncertainty of the process often leads manufacturers not to report suspected or verified breaches, especially in systems used on the factory floor. Many states have laws requiring companies to report breaches in their networks, but only when those breaches involve compromise of personal data; none require reporting of breaches that may have deleterious impact on the operation of systems, including ones used in manufacturing. When reporting a cyber incident in response to the requirements in DFARS Clause 252.204-7012, contractors/subcontractors submit to DoD—

- A cyber incident report via <https://dibnet.dod.mil/>
- Malicious software if detected and isolated
- Media or access to covered contractor information systems and equipment when requested by the requiring activity/contracting officer

Using the NIST SP 800-37, discussed above, it may be possible to modify existing published guidelines and requirements to include protections for the factory OT environment. Documents that may be amended include:

- NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*
- DFARS Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
- DHS Cybersecurity Information Sharing Act of 2015

## Defense Federal Acquisition Regulation Supplements

On October 21, 2016, DoD published a Final rule amending the Defense Federal Acquisition Regulation which specifies requirements for Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-Do18). The information specified is designated as “covered defense information.” which includes controlled technical information or other information as defined in the Controlled Unclassified Information (CUI) Registry. DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, outlines categories requiring safeguarding. Parts A and B of this regulation indicate that technology used in manufacturing should be protected and cyber incidents reported; however, as in the case of many other regulations, directives or guidance currently available, only IT is specifically mentioned in the discussion of systems requiring protection.

These regulations and other current DoD regulations will have limited benefit to protect DoD interests specifically against IIoT cybersecurity risks. The DFARS provides a standardized/uniform set of requirements for all covered defense information security needs. Contractors may not understand that CDI includes sensitive factory data. The focus is protection of information on ICT systems. Contractors may not address cybersecurity of Industrial Control Systems (ICS). Frequently, IoT gets

added to the ad-hoc networks on the manufacturing floors, creating an unsecured vector into the factory's network.

### DHS Cybersecurity Information Sharing Act of 2015

The Cybersecurity Information Sharing Act of 2015 was “intended to build upon previous Department of Homeland Security efforts to have businesses and other agencies share information with the federal government about hackers and cyber intrusions so they can all be more adept at thwarting network attacks.”<sup>49</sup> However, many small businesses have struggled with the process and cost of entering the program; hence, few participate. Once the process is streamlined, participation may increase.

Companies that are reporting data breaches often do so through US-CERT (<https://www.us-cert.gov/>). However, fear of additional regulation, deterioration of reputation, and similar concerns lead many companies to underreport data breaches – or not report them at all. Most companies that have plans in place for dealing with a breach can ride through the breach exposure easier than those that try to hide a breach. Training a company's security personnel is key in assuring they will respond appropriately to data breaches. For DoD, companies that are reporting cyber incidents in response to the terms and conditions of their contract, DFARS Clause 252.204-7012, are required to report directly to DoD at <http://dibnet.dod.mil>. Because cyber incidents of OT systems in manufacturing centers producing items for DoD can have unique impact on the nation's military operations and security, manufacturers who have DFARS Clause 252.204-7012 in their contract that includes covered defense information are required to report cyber incidents directly to DoD at <http://dibnet.dod.mil/>.

### Areas for Further Research & Development

The CFAM JWG believes that cybersecurity in manufacturing may be improved by future efforts to cooperate in understanding the nature of the threat and developing the means to prevent cyber-attacks on the manufacturing process. These efforts include:

- Working with the DHS Information and Sharing Organizations (ISAOs) and Manufacturing ISAC to gain insight into the threat environment and attack vectors to address priority weaknesses on the manufacturing floor.
- Exploring laws relevant to patent and trademarks and potential courses of action for legal protection for companies involved in defense manufacturing.
- Exploring opportunities to expand the NIST Cybersecurity Framework to include systems protection needed on the manufacturing floor.
- Exploring opportunities to extend existing standards to address cyber considerations on the manufacturing floor.

---

<sup>49</sup> Kristen Torres, “Small businesses face hurdles joining DHS cybersecurity program.” *Bloomberg News.com*, 17 June 2016. <https://about.bgov.com/blog/small-businesses-face-hurdles-joining-dhs-cybersecurity-program/>

## Findings and Recommendations

In summary, the JWG found:

- No DoD policies or regulations have been developed specifically for cybersecurity in the manufacturing OT environment; nevertheless, guidance that applies to the IT environment may be adapted to the OT environment.
- Cyber incident reporting is currently hindered by companies concerned with sharing their data. Therefore, developing a reporting method that allows companies to feel comfortable sharing this information will provide DoD and the NDIA a more efficient and effective method of learning about trends in attacks.
- Cybersecurity is a growing concern for manufacturers and their customers; hence, communicating consistent guidance and training as this issue gains traction can provide the greatest impact for securing the manufacturing process from cyber threats.

## APPENDIX D : REPORT OF CFAM JWG TEAM ON TECHNOLOGY SOLUTIONS

Building on the recommendations from the previous NDIA study, the NDIA CFAM Technology Solutions (TS) Team was established to address the following questions:

- What technical solutions can be identified, either available now or under development, to increase cybersecurity in the manufacturing environment?
- What new technology-based concepts should be explored?

To complete their task, the Team first analyzed specific threats within the current environment so that proposed solutions might be directly applicable to manufacturing and feasible with few (or no) significant modifications to available technological resources.

### Threat Analysis

The Technology Solutions Team developed three sample case studies based on representative manufacturing scenarios (summarized in Figure 16). Readers are cautioned that these case studies are illustrative rather than comprehensive.

CASE STUDY	SCENARIO	PRIMARY THREAT FOCUS
<b>Confidentiality</b>	Computer numeric controlled (CNC) machining	Intellectual property theft
<b>Integrity</b>	Metal additive manufacturing	Compromised part quality
<b>Availability</b>	Environmentally controlled, hazardous process	Compounded system of systems safety vulnerability

*Figure 15: Representative Manufacturing Case Studies for Attack Tree Analysis*

For each case study, attack trees were developed, illustrating remote, local, and physical attack vectors. A summary of threats and impacts is shown in Figure 16.

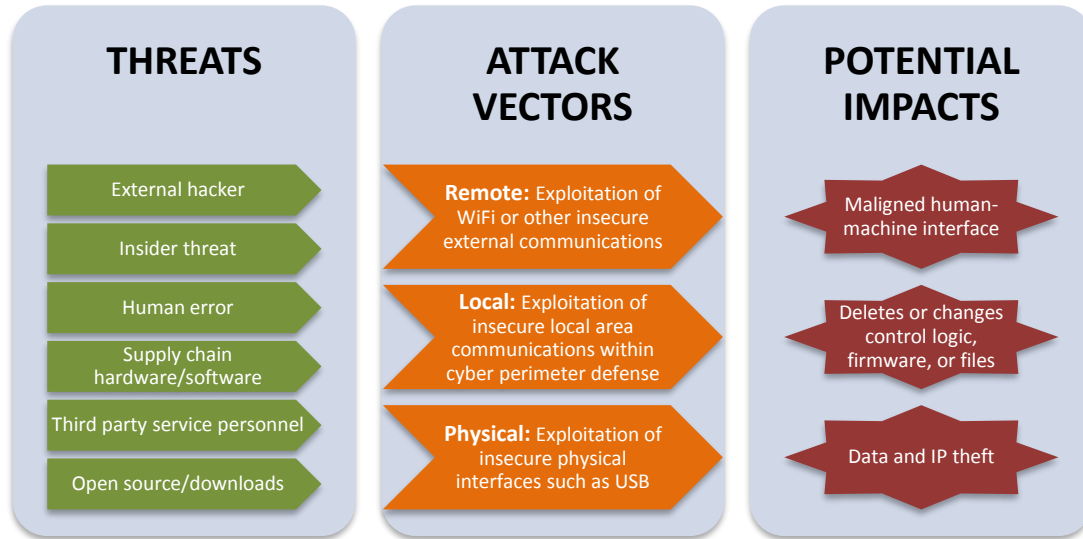


Figure 16: Threats – Attack Vectors – Potential Impacts

Potential vulnerabilities identified for the three case study scenarios include:

- Lack of secure storage;
- Use of default passwords;
- Lack of efficient techniques at the control system to detect unwanted logic or compromised files/models/parameters;
- Lack of techniques to test the quality of input files;
- Lack of cryptographic techniques or the use of weak cryptography algorithms;
- Lack of secure communication (authenticated) protocols;
- Weak authentication credentials or keys used;
- Inadequate network segregation;
- Insecure configuration of OS and applications;
- Poorly configured and unsecure interfaces or ports;
- Lack of proper account management;
- Lack of role based access control and authentication;
- Lack of “non-repudiation” (ability to securely keep a record of the actions performed by the operator on the design files);
- Read and Write access to memory provided with no authentication;
- Lack of audit reports; and
- Lack of secure boot and run time integrity checking.

## Available Solutions

A defense-in-depth security architecture is based on the premise that any one point of protection may, and probably will, be defeated. The ISA-99 Industrial Automation and Control Systems Security in Manufacturing architecture recommends using multiple layers of defense focusing on physical, network, computer, application, and device security.

Figure 18 depicts a notional enterprise and industrial network, including the interface to the building automation and control network. Based upon this diagram, mitigation strategies first consider the human dimension and business processes that could be put in place to reduce risks. Technologies to further mitigate risk and a resulting gap analysis are described, noting that in this example improved setup of the wireless access point may be adequate to foil certain types of attack. However, layered security at the field device end points, which would provide a substantial improvement, were not implemented in this case.

## Business Process Solutions

Basic cyber hygiene and best practices adopted from IT and addressed in existing and pending NIST cybersecurity guidelines may be the “low hanging fruit,” but some of these measures will require a significant culture change on the shop floor, including, but not limited to:

- Reducing/eliminating shared accounts, and allowing named user access only.
- Limiting access and change capabilities based on user accounts.
- Ensuring controller consoles lock after a period of inactivity where possible.

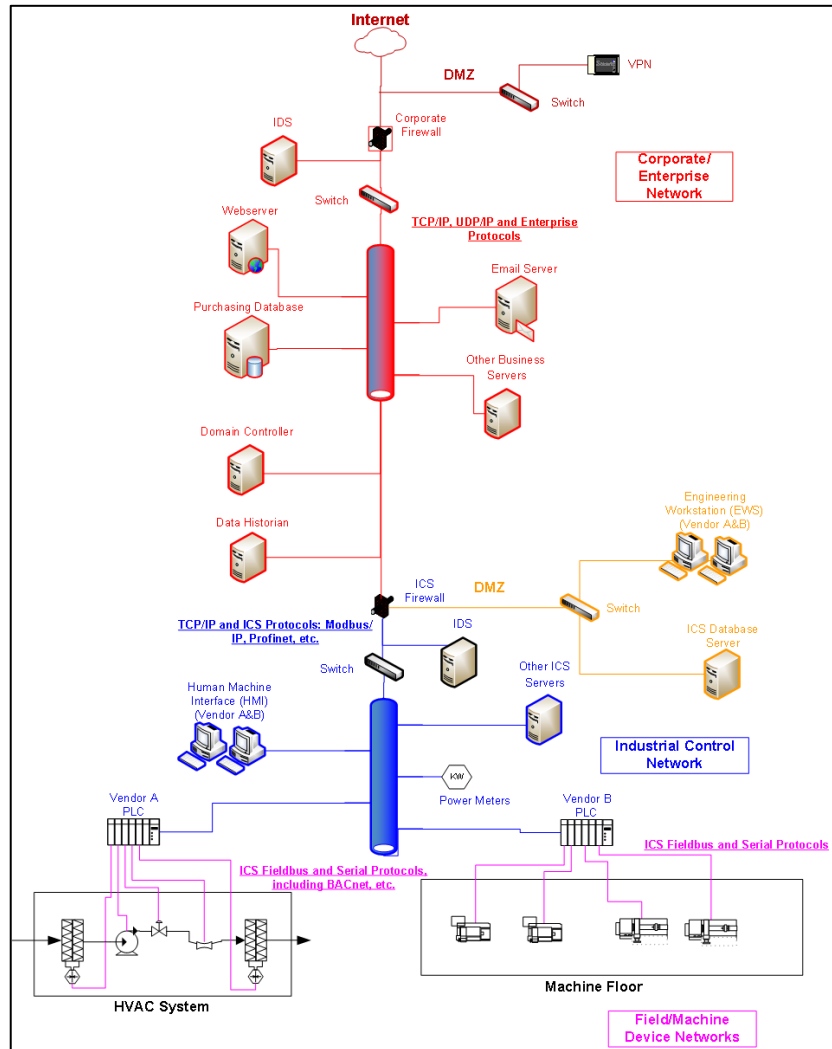


Figure 17: Case Study Reference Architecture

- Restricting network access, to include the ability to move to and from the Internet and other internal sub-nets. No external access should be allowed for third-party vendors unless initiated by the company (never by a vendor alone or automatically).
- Conducting regular reviews of operating systems and applications for security updates from the software manufacturer.
- Disabling external drive/USB auto-run where possible.
- Forcing password changes.

Enabling operators to be key partners in cyber defense is critical but will require training and collaboration to achieve the buy-in necessary to change current mindsets and practices. To overcome human dimension challenges, cybersecurity professionals must understand and address viable shop floor concerns and priorities to improve adoption of both basic cyber hygiene and near- and long-term technology solutions. In addition, response to an anomalous condition can be either human- or technology-based – or both. Historically, operators have been trained to assume failures are due to physical conditions. As current ICS technologies lack awareness of cyber-related failures, operators can benefit from training that enables them to recognize that a problem may not be due to a physical failure. For example, operators could do the following to recognize potential cyber-related failures:

- Perform a local evaluation to confirm/deny agreement with what the ICS indicates. In manufacturing operations, such procedures do not normally exist; and
- Evaluate other operations that require a control action from the same part of the process. For example, in a man-in-the-middle attack, the attacker would not likely address all traffic with the expected responses. If the anomaly is not characteristic of normal physical failures, there is likely a good reason. The attacker may not understand the configuration as well as the plant operators and engineers, and so may not recognize how to address oddities propagated by the attack.

It is essential that operations and network security personnel develop a good working relationship and increase interaction. In some cases, the network security may be an independent integrator, yet the more the network security personnel understand about operational priorities and consequences, the better they are able to improve both security and system performance, thereby leveraging the company's capital investment. In addition, when unfamiliar anomalies occur, they can be involved in recognition and response.



### *Technology Solutions*

The following solutions may be common for IT but not for OT and ICS:

- Security appliances
- Firewalls in use between enterprise and control system networks, and properly configured to allow only the necessary traffic to/from the control system network. A demilitarized zone (DMZ) is part of proper configuration and vetting communications.
- Intrusion detection systems (IDS) that are properly configured for ICS-specific protocols like BACnet and ModBus, but also designed to use both anomaly and signature-based methods.
- ICS configuration
- Application of multi-factor logic and sensing to validate application of more advanced logic before applying complex operations.
- Data protection
- Consistent use of hashing or signature verification techniques to ensure the integrity or origin of design files as they are exchanged person to person or person to machine

Long-term solutions include:

- Integrating well-recognized cyber defense mechanisms on proprietary networks and digital buses
- Installing firewalls, segmentation, and sensing of ICS proprietary networks, buses and hosts
- Correlating IDS distributed across the facility for enhanced state awareness
- Developing secure solutions for legacy systems (bump-in-the-wire) and integration of security protocol advancements
- Installing “sentinel” systems that seek and inhibit “illogical control behavior”
- Employing new sensor modalities for advanced attack detection to prevent subversion of security technologies by an attacker
- Improving ICS configurations
- Initiating off-normal physical reporting in conjunction with cyber detection mechanisms
- Combining physical and cyber technologies for efficient detection
- Creating a system of hardware-based mutual authentication
- Protecting data
- Initiating a system to provide an automated, robust comparison of file data/file version against an approved reference file

## Emerging Solutions

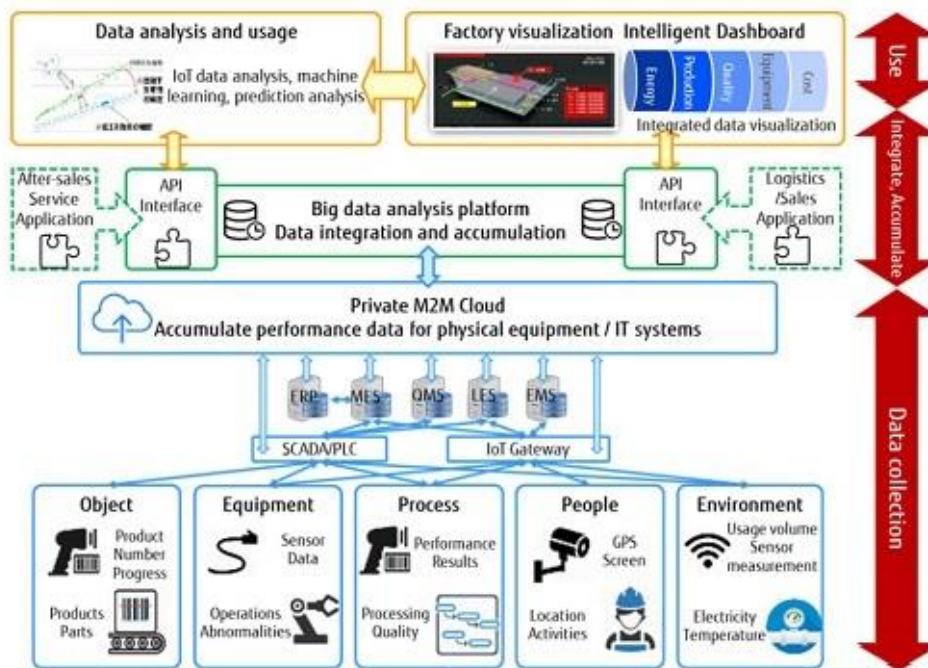


Figure 19: Smart Manufacturing Technology Convergence

While many manufacturers will have to address cybersecurity challenges associated with legacy systems or mixed conventional and digital environments for decades to come, new manufacturing facilities have the advantage of being able to design operational and business processes to address cybersecurity from the ground up. These smart

manufacturing environments will leverage enterprise-wide integration of data, technology, advanced manufacturing capabilities, and cloud and other services with new business models as shown in Figure 20. These technological developments are enabling product innovation, process efficiencies, customization, collaborative and/or distributed production, and other new modes and business models. However, strategies are still needed to comprehensively address security challenges brought about by this new industrial revolution as these opportunities are revolutionizing attack capabilities as well.

Securing smart manufacturing assets requires a comprehensive security model based on a well-defined set of security policies. Given the human-machine and machine-to-machine interfaces, a robust Security Management Plan must address technology, processes, and people (Figure 19). As security of organizations could be compromised at many layers, it is important to create a single point of contact (individual or office) to coordinate security matters and report incidents. Solutions are emerging that allow unified reporting

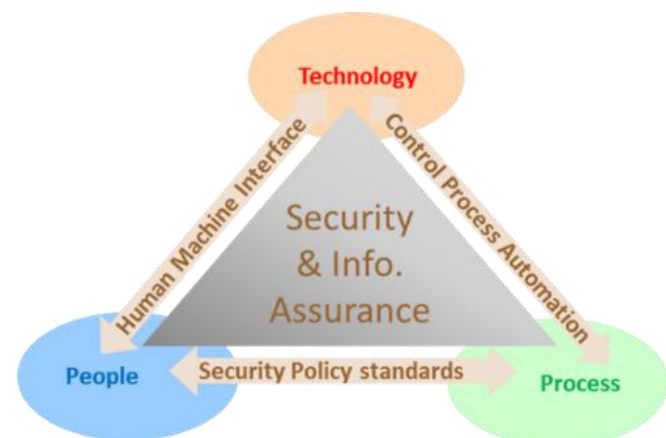


Figure 18: Manufacturing Security Management Plan

to detect any threat to the application, process or network, providing granular visibility of traffic and alerts to deviations from baseline operations and facilitating attack forensics.

Currently, smart manufacturing environments are custom-designed, complicated, expensive, and built on proprietary communications. To achieve affordable plug-and-play capabilities, next generation hardware and software technologies must work together through common security and communication standards. Standardization would lower the cost of entry to smart manufacturing for S&ME. In addition, as more cloud technology and internet connectivity is leveraged toward the Industrial Internet of Things (IIoT), it becomes imperative to assure the identity of the “things” in order to have secure exchanges of information. The IT to OT integration issue is solvable but needs standards of secure communication to leverage the Internet as the main gateway.

A distributed global manufacturing ecosystem increases the challenge of intellectual property (IP) protection. Engineers and operators are no longer under one roof but in different physical locations or countries. The process of black-boxing IP could be the norm, so that no one entity has total exposure to the full process IP. As vendors shift from providing physical parts to providing digital code that end-users purchase to make parts themselves, new business models and rules for protecting IP will also emerge out of necessity so that, for example, a 3D printer file is not only encrypted for security, but also includes provisions to restrict the number of allowable uses.

Smart manufacturing includes software and sensors that allow for precise predictions of maintenance needs, material demand, overtime, and other factors, based on data captured at all points of production. However, the volume of unstructured data that could be consumed in big-data projects creates new kinds of security challenges and requires a new mindset toward data-centric security measures. Big data is too new for security personnel to understand what constitutes normal behavior. Security professionals need to comprehend the analytics and automation being applied to determine how best to protect a big-data enterprise, because there is not currently any practical way to fully maintain situational awareness of the data at the accelerated rates of acquisition and change. With that level of understanding, organizations and vendors working in big data will continue to evolve their tools, techniques, and best practices, which will benefit smart manufacturing security.

Combining the advantages of big data and mobile devices, augmented reality (AR) is being used with increasing frequency on the shop floor in a number of ways, including as a training aid, maintenance aid, and operational dashboard. While the virtual overlay of information provides many benefits, it also opens up another vulnerable interface. For example, a hacker could compromise the output of an AR system, tricking users into thinking computer-generated objects are real. AR applications require access to a variety of sensor data such as video and audio feeds and geolocation; a malicious application could leak a user’s field of view or location. AR solution vendors must address head-on the potential privacy and security risks that this technology can introduce. Some existing security controls and practices – such as encrypting wireless data transmissions – can serve to protect AR system inputs and outputs. Organizations need to have clear visions about how to overlay their existing security regimes onto the AR field.

## Technology Solutions Recommendations

The Technology Solutions Team carried out research and participated in several interviews with individuals either participating in or closely involved with the advanced manufacturing in industry. The team has extracted a series of recommendations that cover two types of issues facing the DoD and other government agencies in protecting the supply chain for the DIB. Not only is it necessary for large primes to succeed in their

efforts to have a secure infrastructure; S&ME are also critical to the success of efforts at improving cybersecurity. Moreover, this group requires more immediate attention; their limited capabilities and resources create a significant gap in supply chain integrity. Unfortunately, the small to mid-sized players are less well-equipped to support implementation of even current cyber controls and infrastructure required to minimize potential breaches, often due to their lack of capital and expertise.

### Selected R&D Recommendations



Figure 21: Summary of R&D Recommendations

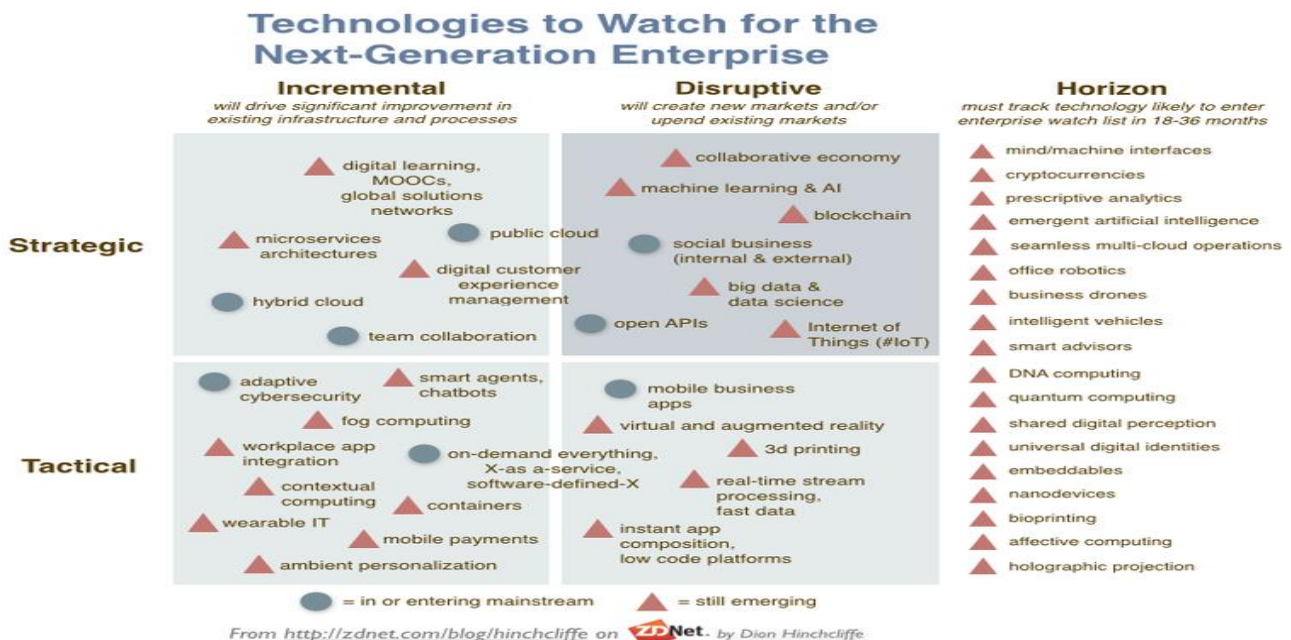


Figure 20: Emerging Enterprise Technologies



**Recommendation 1:** The Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD (SE)) should sponsor development of an agile and flexible threat deterrent system, designed to aid S&ME who represent a significant sector of the DIB supporting large primes in delivering mission-critical equipment. The outcome should effectively provide ‘plug-in’ modules (hardware and/or software) to counterbalance the threats in both the IT and OT environments. In effect, this approach would replace the traditional ‘air-gap’ that sufficed before the digital thread became part of the operational architecture. In this way, a protective boundary will exist, and continuity of production would have the necessary systemic robustness and integrity. This goal can be obtained by:

- Ensuring widespread understanding that MEP exists to support small to mid-sized manufactures, and that guidance exists in the NIST Cyber Security Framework, which outlines a methodology to I (Identify), P (Protect), D (Detect), R (Respond) and R (Recover) from cyber-attacks.
- Accelerating deployment and use of the process proposed in Securing American Manufacturing (SAM), an initiative already sponsored by the ODASD Office of the Assistant Secretary of Defense for Manufacturing and Industrial Base Policy (ODASD (MIBP)); promote education on DFARS and develop an outcome ‘alert’ system to provide awareness to manufacturers associated with the DIB who may be most vulnerable to cyber-attacks; assure that the proposed ‘alert’ system is not penalty-based to avoid resistance by those most in need of participating.
- Initiating a new program that effectively combines the outcomes from several programs now in progress or near completion in the advanced research projects agencies, for example: IARPA’s CAUSE (Cyber-Attack Automated Unconventional Sensor); DARPA’s VETS (Vetting Commodity IT software and firmware); DARPA’s RADICS (Rapid attack detection, isolation and characterization), which can be employed in conjunction with the Mitre Corporations’ ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), which is used to characterize and describe post-compromise adversary behavior in an enterprise network. Combining elements from these efforts into an overarching system to deliver an appropriate ‘plug-in’ intermediary module could provide relevant and necessary protection of the Enterprise (IT/OT) hardware and/or software systems.

**Recommendation 2:** The Offices of the Under Secretary of Defense, Acquisition, Technology and Logistics (USD (AT&L)), Chief Information Officer (DoD CIO), Office of the Assistant Secretary of Defense (Research & Engineering) (OASD(R&E)) and Office of the Assistant Secretary of Defense for Logistics & Materiel Readiness (OASD(L&MR)) should sponsor a review of commercial solutions to identify Enterprise Architecture and new technology concepts for S&ME that are affordable and easily adaptable to integrate them seamlessly into the defense supply chain and mitigate continually changing threats. This recommendation may be accomplished by:

- Identifying and deploying new technologies that are likely to improve the way manufacturers represented in Defense Industrial Base (DIB) operate so that their architecture may become

more secure, including adaptive cybersecurity, hybrid cloud, blockchain, artificial intelligence, augmented reality, and others. A benchmark study for these should be sponsored.

- Evaluating cyber-physical models that provide conduits in the architecture at risk (based on ISA99 62443) by rigid penetration testing, with the aim of developing a better understanding of the trade space between physical testing and virtual simulation.
- Reviewing and developing solutions for detecting cyber-attacks based on properties of the part(s) being manufactured.
- Driving small and prime manufacturers toward a robust security platform versus reliance on any one security tool; develop Security as a Service (SECaaS) and enhance Enterprise as a Service (EaaS).
- Encouraging greater use of assistive and Soft Robotics (Artificial Intelligence and Human-Computer Symbiosis Technologies) to prevent human errors while increasing speed and efficiency.

**Recommendation 3:** The Office of the Assistant Secretary of Defense (Research & Engineering) (OASD(R&E)) should sponsor further research to identify the best Data Protection, Design, and Encryption technology that will allow for better control and real-time monitoring suitable for the enterprise. Specific steps to accomplish this goal include:

- Promoting Next Generation Data Protection (NGDP) solutions that are already available for end-to-end security; these are set up by tiered architecture with multilayered protection for data that secures the connections and devices it travels across, from thing to cloud, across the entire manufacturing environment. NGDP integrates data protection such as Data Loss Prevention (DLP), Firewall, Application Control, Identity Awareness, and more into one appliance.
- Assessing advanced sensing machine tools and employing scalable control systems that operate in real time and mitigate vulnerabilities by automated discovery.
- Building advanced data governance technologies, authentication, and Identity and Access Management (IAM) with personalization specific to the enterprise and its metrics.
- Proposing real-time high-speed encryption techniques in wire, in memory, in transit/motion, and on the disk; included would be a recommendation for employment of constructive key management (CKM), a dynamic single-use key management that enhances system security.
- Offering an enhanced mechanism for assuring the availability of systems and affording rapid disaster recovery that ensures business continuity for individual manufacturers and improves the real-time response of third-party vendors offering Disaster Recovery as a Service (DRaaS).

**Recommendation 4:** The Office of the Deputy Assistant Secretary of Defense (Systems Engineering) (ODASD(SE)), Assistant Secretary of Defense for Logistics & Materiel Readiness (OASD(L&MR)) and Chief Information Officer (DoD CIO) should support the transition to the Hybrid Cloud. This offers both platform-as-a-service (PaaS) and Infrastructure-as-a-Service (IaaS) capabilities, and may provide more efficient and effective computation, storage, and networking solutions. These agencies should also encourage Virtualization that will provide private on-premise, enterprise-class IaaS technology. Cloud technology in the wake of Industrial IoT will have to:

- Recognize and prioritize security as a critical design factor for both individual devices and smart manufacturing systems.
- Improve the ability to move data to the hybrid cloud and communicate promptly over an encrypted connection, using technology that permits secure transfer, storage, and processing of data and applications.
- Implement cyber hygiene, Software-Defined anything (SDx), segmentation, and containerization.
- Build a methodology that allows for verification of trust in third-party vendors (e.g. [Google](#), [AWS](#)) supporting small businesses.
- Place all mission-critical applications in a private cloud-based infrastructure for an overarching enterprise (e.g., Nutanix – [www.nutanix.com](#) ) and for enterprise asset management (e.g., Infor – [www.infor.com](#)). Use cloud-base storage for design functions (e.g., On Shape, the first and only fully cloud-based 3D CAD system, [www.onshape.com](#) ) and for control and optimization (e.g., Sig Opt, a cloud-based ensemble of optimization algorithms, [www.sigopt.com](#)).
- Deploy collaborative robots to assist and support humans to reduce the emphasis on repetitive processes and intensive labor; these robots are being developed by such groups as Stanley Robotics ([www.stanleyinnovation.com](#)) and Symbio Robotics ([www.symbio.io](#)).

**Recommendation 5:** The Offices of the Under Secretary of Defense, Acquisition, Technology and Logistics (USD/AT&L), and Office of the Assistant Secretary of Defense (Research & Engineering) (OASD(R&E)) should develop guidance that helps manufacturers take into account greater automation, with investment driven by the next wave of the Emerging Advanced Manufacturing trends: accelerated production cycles, advanced technology, social, mobile, analytics, security, and changing labor demographics. Several important factors must be considered when developing this guidance:

- *Social media* savvy consumers are forcing manufacturers to become more customer-centric and deliver products on demand. Challenges in *secure mobility* and *unified communications* will have to be addressed.
- The *Industrial Internet Of Things* allows for condition-based maintenance, which is driving efficiencies as businesses save on labor and service costs.



- A more *technically proficient labor force* will be required to manage supply chain operations. Both workforce skills and business practices must be retooled by turning to new technology, including smart glasses and *Augmented Reality*.
- *Big data* is too new for security personnel to understand what constitutes normal behavior. Security professionals need to comprehend the analytics and automation being applied to determine how best to protect a big-data enterprise.
- *Virtualization* and the virtual machines that permit manufacturers to run multiple operating systems and applications on a single physical server will need to be considered.



## APPENDIX E : CYBERSECURITY FOR ADVANCED MANUFACTURING JOINT WORKING GROUP TERMS OF REFERENCE

### Terms of Reference

#### **Cybersecurity for Advanced Manufacturing (CFAM)**

*A study by a Joint Working Group of Government representatives  
and members of the National Defense Industrial Association (NDIA)*

#### **Objective**

Government and industry members of the Cybersecurity for Advanced Manufacturing (CFAM) joint working group (JWG) will work collaboratively to build on the recommendations in the 2014 NDIA white paper, *Cybersecurity for Advanced Manufacturing*. The CFAM JWG will identify the types and boundaries of cybersecurity threats, vulnerabilities, and consequences in the manufacturing environment and define actions to mitigate those risks. The CFAM JWG will identify ways to incentivize and assist manufacturers (particularly small and medium enterprises (S&ME) in defense supply chains) to improve cybersecurity in manufacturing systems by evolving policies and contract requirements, enhancing security practices, and offering industrial / contractor workforce cybersecurity training. Implementation plans will be developed for the updated courses of action.

#### **Background**

In 2014, NDIA's Manufacturing Division and Cyber Division jointly developed a White Paper to heighten awareness of the emerging threats, vulnerabilities and consequences in the Industrial Control Systems used in manufacturing, with special attention on defense systems manufacturing. The paper outlines the findings of a 12-month study of the threats to manufacturing specifications and technical data transiting or residing in manufacturing systems, alteration of the data (thereby compromising the physical parts produced), or interference with reliable and safe operation of a production line. The NDIA joint working group recommended actions to better protect the digital thread through which defense systems' unclassified technical information flows during the manufacturing process. Undersecretary of Defense for Acquisition, Technology & Logistics, Frank Kendall, endorsed the recommendations and designated Principal Deputy Assistant Secretary of Defense for Systems Engineering, Kristen Baldwin, to serve as the government sponsor to continue the work.

#### **Scope**

Review and update actions recommended in the 2014 NDIA white paper, *Cybersecurity for Advanced Manufacturing*, to better protect the digital thread that drives defense systems' manufacturing. Develop implementation plans for the updated courses of action that have been coordinated between government and industry.

#### **Specific Tasks**

The CFAM JWG will form teams to analyze the multiple facets of manufacturing cyber threats, vulnerabilities, and consequences in the defense industrial base and develop recommendations for

actions that will better protect the digital thread. Questions the joint working group will address include:

- What defines a manufacturing environment for the defense industrial base (i.e. within and among the members of defense supply chains)? What are the cybersecurity threats, vulnerabilities, and consequences? How can the cybersecurity risks in manufacturing environments be identified and mitigated?
- What use cases are important across the life cycle of the manufacturing environment? What conditions and practices contribute to cybersecurity or increase cyber risks?
- What actions and activities can improve cybersecurity in the manufacturing environment? What are the activities with the potential to have the greatest near-term impact?
- What types of education, training and awareness of cybersecurity for manufacturing environments are required for existing and future workforces, including workforce leadership? How can cultural and behavior change contribute to increased cybersecurity?
- What existing policies regulations, and standards are applicable to cybersecurity in advanced manufacturing? How do existing policies, regulations and standards need to be augmented, and by whom?
- How can existing network breach reporting and communication processes be improved to increase cybersecurity in manufacturing environments, and by whom?
- What activities implemented inside and outside the Department of Defense, other government agencies or by the private sector can be leveraged to better protect manufacturing networks?
- What technical solutions can be identified, either available now or under development, to increase cybersecurity in the manufacturing environment? What new technology-based concepts should be explored?

### ***Deliverables***

The CFAM JWG will issue a report by December 2016 for further coordination within DoD and other Government agencies as appropriate.

### ***Study Organization***

Melinda K. Reed, Deputy Director for Program Protection, Assistant Secretary of Defense, Research and Engineering (ASD(R&E)) will serve as the government lead in this activity; Catherine J. Ortiz, President, Defined Business Solutions LLC, will serve as the industry lead. The CFAM JWG member list is shown as Attachment A and will be updated as needed. Team members may be added throughout the activity as subject matter experts are identified to contribute to the work.

## APPENDIX F : DEFENSE MANUFACTURING ENVIRONMENT DIAGRAM NARRATIVE

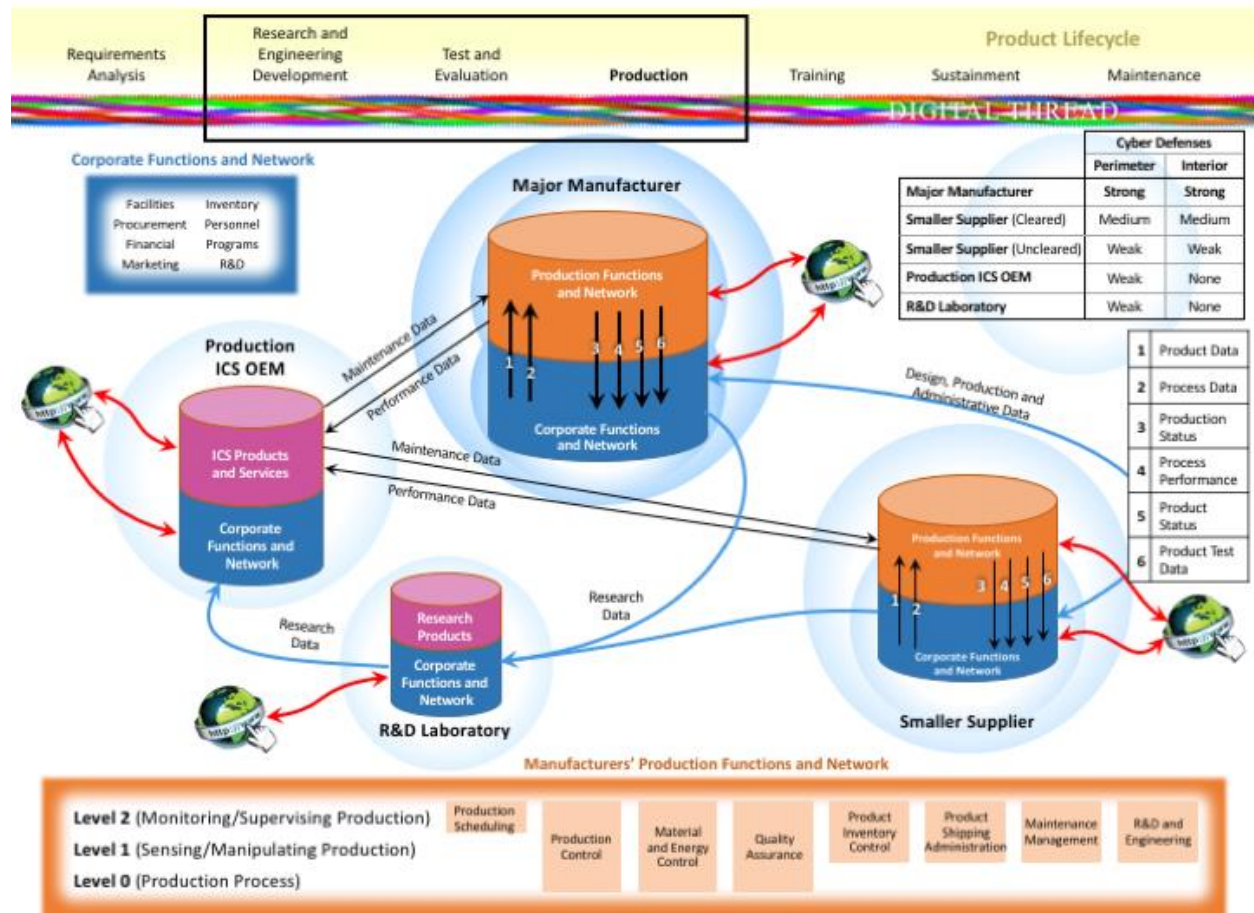


Figure 22: Defense Manufacturing Environment: Production

### PRODUCTION

This slide illustrates what we call the “Digital Thread.” The digital thread is the set of digitally created, stored and exchanged information that supports the manufacturing and sustainment processes of modern products. The digital thread exists throughout the product lifecycle, which is shown across the top of the slide.

1. Assume the existence of a major manufacturer or system integrator. This firm has a set of corporate (blue) and production (tan) functions that are supported by one or more networks. In general, corporate functions and the networks that support them include those listed in the box in the upper left corner of the slide.
2. The major manufacturer is supported by one or more R&D Labs, with whom they exchange research data.
3. The major manufacturer works with one or more smaller suppliers, with whom they share design, production and administrative data, and which may also be connected to some of the R&D labs.

4. The major manufacturer and related suppliers leverage Industrial Control Systems and related ICS maintenance services provided by one or more OEMs. The OEM's clients receive Maintenance Data and Services and provide ICS performance data to the OEM to support current maintenance activities and future product improvements. The OEM may also receive research data from the R&D Lab to support development or refinement of the OEM's products.
5. Each of the organizations is connected to the Internet and has perimeter cyber defense capabilities.
6. The major manufacturer uses a segmented architecture that provides separate internal cyber defense capabilities for its corporate and production networks (darker blue bubbles). The smaller supplier has interior defenses for its corporate network, but its architecture is not segmented and its production network may lack a separate set of defense capabilities.
7. In general, we categorize the efficacy of the cyber defenses at a high level as shown in the box in the upper right side of the slide.
8. Within each firm, data may be exchanged between the corporate and production networks (for simplicity, we show these exchanges in only the major and smaller suppliers). The general types of data are listed in the box on the right side of the slide.
9. Finally, we see a three-level decomposition of the functions that may be executed in the production networks. This list was extracted from the Supporting Activity Model in ISA 95. In terms of cybersecurity, these functions represent portions of the manufacturing process that could be adversely affected by cyber-attacks.

Red stars containing letters show potential attack points used in each use case. Also, red lettering in the large box at the bottom of the slide indicates production functions that may serve as targets and may be adversely affected by cyber-attacks.

#### Confidentiality Use Case:

- A. Adversarial insider with authorized access to production and test equipment.
- B. Theft of data from CAD/CAM workstations by malicious 3rd party exploiting insecure external communications and vulnerabilities of perimeter cyber defense.
- C. Theft of data on-site from CAD/CAM workstations by malicious 3rd party exploiting insecure local area communications (within cyber perimeter defense).
- D. Embedded sensors within manufacturing equipment containing malicious hardware/software capable of transmitting data to an external location.
- E. Theft of data by visitors (specifically maintenance personnel) with extensive or unsupervised access to manufacturing equipment.

**Integrity Use Case:**

- A. Rogue designers inserting malicious logic into the CAD model, .STL file or Tool command file.
- B. 3rd party models or files embedded with unwanted logic.
- C. Malicious 3rd party CAD/CAM software that inserts extraneous or deletes logic into the models/files
- D. Tamper models/files/control parameters via Malware infection (by exploiting insecure external communications and software vulnerabilities of CAD/CAM software or operating systems)
- E. Modifying files or process control parameters by exploiting insecure local area communications
- F. Update controller firmware by exploiting insecure physical interfaces such as USB

**Availability Use Case**

- A. Malicious 3rd party performed reconnaissance to find available Wi-Fi signals emanating from a facility
- B. Malicious device inserted through Wi-Fi to BACnet
- C. Modification to smart damper identity performed via malicious device
- D. M Control signal to exhaust damper modified to drive closed
- E. Malicious device replaces smart damper as interface to human machine interface
- F. Autonomous system reacts as programmed to loss of damper



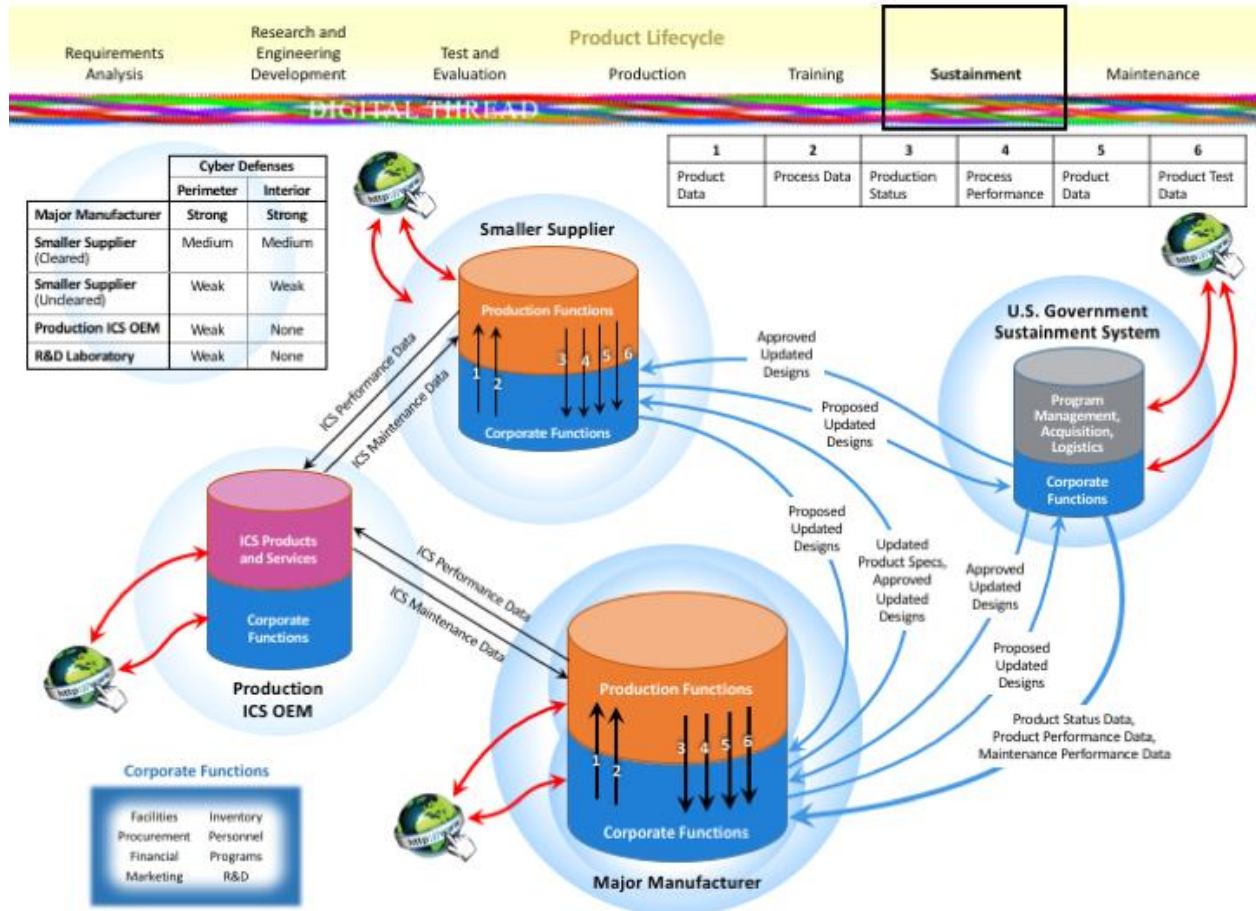


Figure 23: Defense Manufacturing Environment: Sustainment

## SUSTAINMENT

This slide illustrates what we call the “Digital Thread.” The digital thread is the set of digitally created, stored and exchanged information that supports the manufacturing and sustainment processes of modern products. The digital thread exists throughout the product lifecycle, including sustainment, which is shown at the top of the slide.

1. Assume the existence of a major manufacturer or system integrator. This firm has a set of corporate (blue) and production (tan) functions that are supported by one or more networks. In general, corporate functions and the networks that support them include those listed in the box in the lower left corner of the slide.
2. The major manufacturer supports the U.S Government Sustainment System, which executes program management, acquisition and logistics functions as well as a set of corporate functions. The government’s sustainment system sends product status data, product performance data and maintenance performance data to the Major manufacturer, which responds with proposed updated design data. In response to these, the Major Manufacturer submits proposed design updates and receives approved, updated designs from the Government.



3. Both the major manufacturer and the Government sustainment system work with one or more smaller suppliers. The smaller supplier sends proposed updated designs to the Government and the major manufacturer, as needed, and receives approved updated designs.
4. The major manufacturer and related suppliers leverage Industrial Control Systems (ICS) and related ICS maintenance services provided by one or more OEMs. The OEM's clients receive Maintenance Data and Services and provide ICS performance data to the OEM to support current maintenance activities and future product improvements. The OEM may also receive research data from the R&D Lab to support development or refinement of the OEM's products.
5. Each of the organizations is connected to the Internet and has perimeter cyber defense capabilities.
6. The major manufacturer uses a segmented architecture that provides separate internal cyber defense capabilities for its corporate and production networks. The smaller supplier has interior defenses for its corporate network, but its architecture is not segmented and its production network may lack a separate set of defense capabilities.
7. In general, we categorize the efficacy of the cyber defenses at a high level as shown in the box in the upper left corner of the slide.
8. Within each firm, data may be exchanged between the corporate and production networks (for simplicity, we show these exchanges in only the major and smaller suppliers). The general types of data are listed in the box in the top right corner of the slide.
9. Ideally, we would have a decomposition of the functions that would be executed in the sustainment networks, and that model would mirror the Supporting Activity Model in ISA 95. In terms of cybersecurity, such functions would represent portions of the manufacturing process that could be adversely affected by cyber-attacks.

## APPENDIX G : THREAT USE CASES

### Availability Use Case in Cybersecurity: HVAC Compromise and How Complex Controls Magnifies Event

**Description:** Heating, Ventilation and Air Conditioning (HVAC) Malicious Component Failure –Selective Man-in-the-Middle attack that leverages autonomy to magnify impact to a facility.

A facility that is producing hazardous substances has an advanced HVAC system for regulating pressures within the building. By maintenance of pressures with the most hazardous areas at the lowest pressure and normally occupied spaces at the highest, the migration of hazardous substances can be prevented. The system design also uses supervisory control, in that a neural network design implements night-time setbacks increases the air conditioning set points to reduce overall energy usage. The primary temperature and differential pressure control on the system are through some form of PID algorithm, with each hazardous zone having its own controller and separate temperature controllers for the hazardous and occupied zones. Intake and discharge ducting and blowers are common for the hazardous and occupied spaces, but each area has an individual header. In the case of the hazardous areas, high efficiency filters are used to remove pollutants.

During the morning before the workers arrive, the exhaust airflow from the facility gets largely blocked due to an abnormal failure of a damper. While initially unrecognized, this failure was caused due to selective man-in-the-middle attack on the smart actuator, causing the actuator to assume its failure state. The attack was initiated through connection at the facility boundary to a wireless access point on the BACnet and a spoofing device. As this is a man-in-the-middle attack on the damper, the operator did not have a remote indication of any damper failure and is unable to characterize why the HVAC system is misbehaving. However, because of the autonomy involved with this HVAC control system, the malicious actor could indirectly impact several control systems devices. Referring to these impacted devices highlighted in red in the figure, the malicious actor need not orchestrate complex attacks when the control system has the interdependencies necessary to achieve a cascading consequence.

The failure of the damper creates a back pressure on both the hazardous and occupied zones of the facility. In response to the reduced airflow, the inlet damper of each hazardous zone closes to maintain the required differential pressure. However, minimum facility flows are not maintained and the damper controls are not able to equalize consistently, allowing periods where potential migration of hazardous species may occur. In addition, the drop-in airflow prevents cooling and allows the temperature to increase in both the occupied and hazardous areas. As the airflow through the air conditioning coils has dropped, the PID controller continues to increase the amount of coolant to the coils until they freeze—which the freeze protection switch, or freeze stat, fails to prevent due to improper positioning. The regime that the facility is now operating within has also gone outside of the training for the neural network, but as the occupied period is reached, the neural network decreases the temperature set points without regard to the abnormal situation.

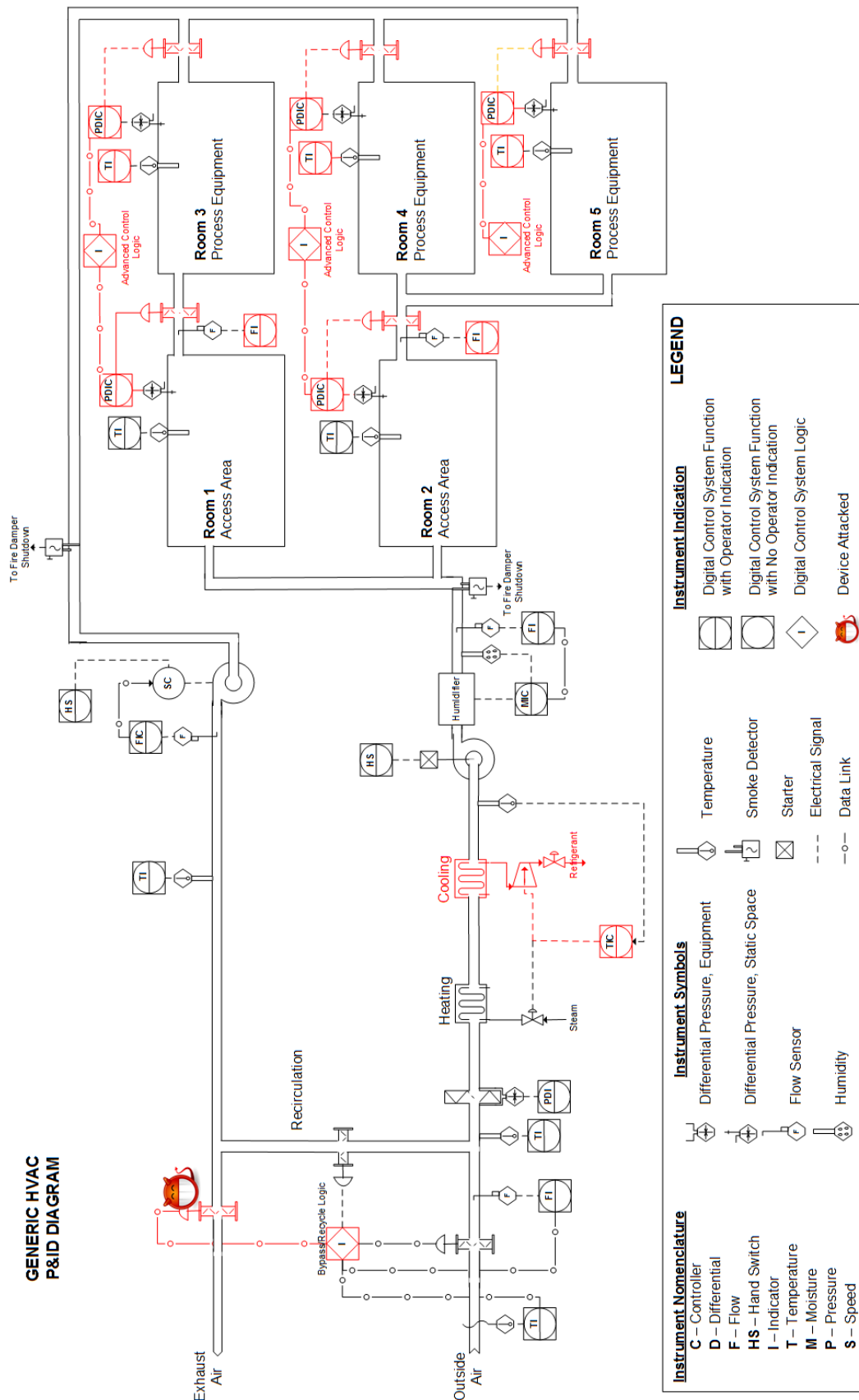








Figure 24: Generic HVAC Diagram

**Goal:** Attack the HVAC in a manufacturing facility to extract the maximum impact to availability with the minimum amount of effort.

**Layers:** Control signal maliciously manipulated via a digital signal, emulating those used for diagnostics and calibration; smart damper identity

**Attack Vectors:**       Remote       Local       Physical

-  Malicious 3<sup>rd</sup> party performed reconnaissance to find available Wi-Fi signals emanating from a facility
-  Malicious device inserted through Wi-Fi to BACnet
-  Modification to smart damper identity performed via malicious device
-  Malicious device replaces smart damper as interface to human machine interface
-  Control signal to exhaust damper modified to drive closed
-  Autonomous system reacts as programmed to loss of damper

## Integrity Use Case in Cybersecurity: Additive Manufacturing Compromise

**Description** – Coordinated attacks aimed at compromising the quality/integrity of additively manufactured parts.

In this use case a small manufacturing firm uses additive manufacturing (AM) to produce parts for both the commercial and defense markets. The AM machine is networked so that CAD engineers can send .STL files directly to the production (CAM) work station where the .STL file is converted to a tool command file specific to the type of AM machine being used. In addition to the local network, the AM equipment vendor can access the AM machine remotely to help monitor and troubleshoot operations – this bridge can be switched off.

A coordinated cyber-attack targets the .STL file, tool command file, or the AM process controls. Any resulting changes to a part could cause part failure and/or performance issues. These attacks are attractive to U.S. adversaries because the part alteration can be made in a way that is undetectable by current test methods.

- The .STL file contains all of the information needed to fabricate the geometry of the part. By altering the coordinates of the vertices making up the .STL file, it is possible to alter the resulting manufactured part (and its properties or performance) in one of the following ways: scaling part geometry in one or more axes; adding small protrusions or indents; altering, moving, or deleting one or more vertices to change internal or hidden geometries or create voids; and altering support structures that may affect the quality of the build.
- The tool command file is generated from the .STL file, providing the AM machine with commands for the x, y, z axis controllers as well as deposition (material, laser, etc.) controls. Altering the tool command file can result in the machine depositing material in the wrong location, not depositing material in desired locations, and change the orientation and spacing of individual build layers.
- In addition to the machine commands built into the tool command file, there are additional AM

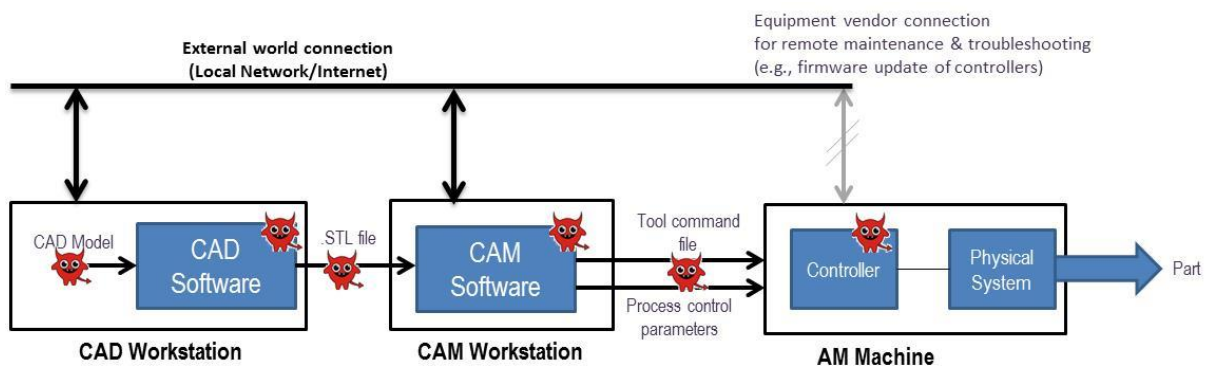








Figure 25: Nominal Simplified Additive Manufacturing Flow

process parameters that are controlled as part of the human-machine interface. An attack on these controls would alter the part build and likely affect part integrity.

**Goal** – Attack the quality of the additive manufactured product

**Layers** – CAD model, .STL/.AMF file, Tool command file, Process Control Parameters, Controllers

**Attack vectors** –  Remote  Local  Physical

-  Rogue designers inserting malicious logic into the CAD model, .STL file or Tool command file
-  3<sup>rd</sup> party models or files embedded with unwanted logic
-  Malicious 3<sup>rd</sup> party CAD/CAM software that inserts extraneous or deletes logic into the models/files
-  Tamper models/files/control parameters via Malware infection (by exploiting insecure external communications and software vulnerabilities of CAD/CAM software or operating systems)
-  Modifying files or process control parameters by exploiting insecure local area communications
-  Update controller firmware by exploiting insecure physical interfaces such as USB

## Confidentiality Use Case in Cybersecurity: Intellectual Property Theft

**Description** – Insider attacks aimed at obtaining critical design/production data that is transmitted to a manufacturing environment.

In this use case, a mid-size US firm manufactures product via CNC machining for both the commercial and defense industries. The industrial control systems, or cyber-physical systems (CPS) utilized by the firm exist on a stand-alone network protected by a perimeter cyber defense. The data of interest consists of CNC control parameters that take the form of G- or M-code files. The firm's CPS machines, which house this data, are networked to each other and have terminals permitting access to production data files for authorized users. After learning that he will soon be laid off, an authorized user attempts to steal several production data files by inserting a company-issued thumb drive into a CPS terminal. This data is then taken to an off-campus network to be transmitted to a firm located in a competing nation.

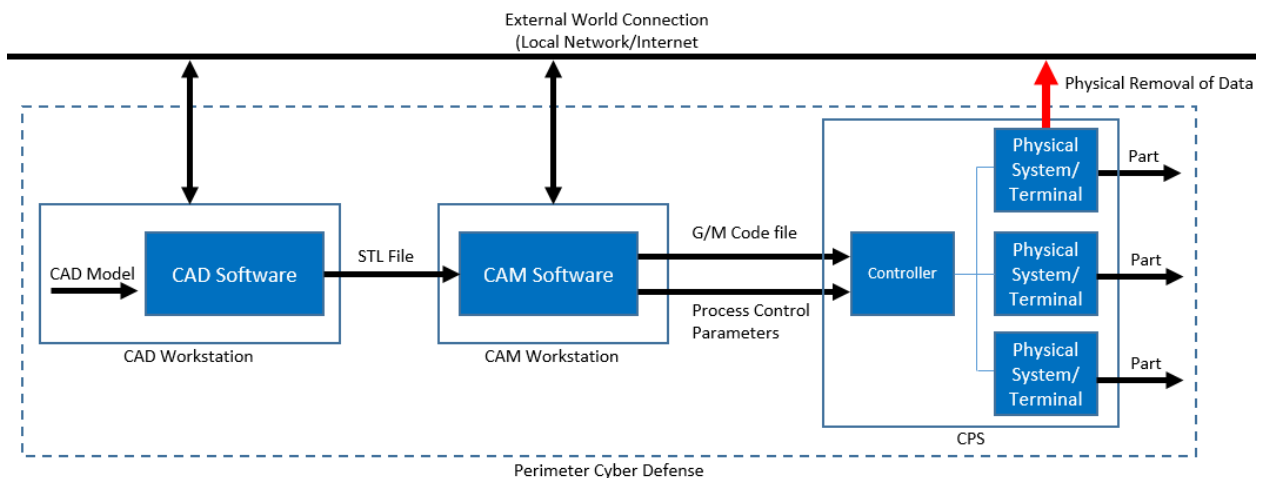


Figure 26: Nominal Simplified Production Data Flow

An insider attack targets the theft of production data files in order to benefit a competitor for personal gain. The loss of this information can lead to the production of counterfeit products and the compromise of fielded defense systems should this information be obtained by a competing nation's intelligence service.

- In an effort to increase responsiveness to rapidly changing production needs, the victim firm provided authorized access to all CPS machine operators. The CPS network does not inhibit the download of production data to authorized devices.
- Since the theft of data was performed by an authorized user, the victim firm may have no record that their CPS network and production data were ever compromised.
- The production data files for the CNC machining process contain the commands for X, Y, Z axis control as well as machine speed and feed rates. This data can be used to not only reverse-engineer a product's design, but also the processing parameters required to machine it.



- By having both design and processing parameters, a competing firm can produce counterfeit equivalents that may be difficult to distinguish from genuine parts. Counterfeit equivalents may look the same but have different performance, adversely affecting fielded defense systems.
- By having critical process control information, the competing firm can incrementally improve the product with minimal cost to gain an advantage over the victim firm. For defense systems, this action can provide an adversary with the ability to develop countermeasures to U.S. technologies.

**Goal** – Compromise critical data (Intellectual Property) for personal gain.

**Layers** – CAD model, .STL file, G/M Code file, Controller, Physical System

**Attack vectors** –

■ Remote

■ Local

■ Physical

- Adversarial insider with authorized access to production and test equipment.
- Theft of data from CAD/CAM workstations by malicious 3<sup>rd</sup> party exploiting insecure external communications and vulnerabilities of perimeter cyber defense.
- Theft of data on-site from CAD/CAM workstations by malicious 3<sup>rd</sup> party exploiting insecure local area communications (within cyber perimeter defense).
- Embedded sensors within manufacturing equipment containing malicious hardware/software capable of transmitting data to an external location.
- Theft of data by visitors (specifically maintenance personnel) with extensive or unsupervised access to manufacturing equipment.

**APPENDIX H : SUBJECT MATTER EXPERTS INTERVIEWED**

Rosalind Bartlett	Defense Procurement Acquisition Policy
Greg Carnevale	Department of Homeland Security
Christian Cowan	Polaris Manufacturing Extension Partnership
Brian Cunningham	PTC, Inc.
Gilliam Duvall	Data Security Strategies, LLC
Marty Edwards	Department of Homeland Security
John Ellis	Defense Contracts Management Agency
John Everett	Defense Advanced Research Projects Agency
Kevin Fischer	Rockwell Collins Incorporated
Michael Fornasiero	UI LABS
Tommy Gardner	Jacobs Engineering Group
Steve Gleason	Micro Craft Incorporated
Mike Gresh	General Dynamics Corporation
Ed Herderick	General Electric Corporation
Gregory Kyle Hoover	Department of Defense Missile Defense Agency
Brian Hughes	Office of Deputy Assistant Secretary of Defense for Systems Engineering
Anthony King	Raytheon Missile Systems
Robert Metzger	Rogers Joseph O'Donnell, PC
George Nickolopoulos	University of Rhode Island
Raymond Richards	Defense Advanced Research Projects Agency
Robert Rolfe	Institute for Defense Analyses
Alex Silva	The Raytheon Company
Russell Smith	Institute for Defense Analyses
Dave Stieren	National Institute of Standards and Technology
Kenneth Sullivan	Micro Craft Inc.
Robert Timpany	Department of Homeland Security
Patricia Toth	National Institute of Standards and Technology
Melinda Woods	Office of the Secretary of Defense, Acquisition, Technology & Logistics, Manufacturing and Industrial Base Policy

**APPENDIX I : TERMS AND ACRONYMS**

3D printing	Additive Manufacturing, or a process of making 3-dimensional solid objects from a digital file
AM	Additive Manufacturing
AR	Augmented Reality
ASME	American Society of Mechanical Engineers
CAD/CAM	Computer-Aided Design / Computer Aided Manufacturing
CDI	Covered Defense Information
CFAM JWG	Cybersecurity for Advanced Manufacturing Joint Working Group
CIA Triad	Confidentiality–Integrity–Availability
CKM	Constructive Key Management
CMS	Critical Manufacturing Sector
CNC	Computer Numeric Control
CPI	Critical Program Information
CPS	Cyber-Physical System
CPU	Central Processing Unit
CUI	Controlled Unclassified Information
DARPA	Defense Advanced Research Projects Agency
DASD(SE)	Deputy Assistant Secretary of Defense for Systems Engineering
DCMA	Defense Contract Management Agency
DDoS	Distributed Denial of Service
DIB	Defense Industrial Base
DFARS	Defense Federal Acquisition Regulation System
DHS	U.S. Department of Homeland Security
DIA	Defense Intelligence Agency
Digital Thread	Bi-directional flow of information connecting departments across the enterprise to increase collaboration and operational agility; enable end-to-end product traceability and improved supplier quality management; and gain visibility into real time performance
DLP	Data Loss Prevention



DMDII	Digital Manufacturing and Design Innovation Institute
DME	Defense Manufacturing Environment
DMZ	Demilitarized Zone
DOC	U.S. Department of Commerce
DoD	U.S. Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DOE	U.S. Department of Energy
DPAP	Defense Procurement Acquisition Policy
DRaaS	Disaster Recovery as a Service
EaaS	Enterprise as a Service
HVAC	Heating, Ventilation and Air Conditioning
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IARPA	Intelligence Advanced Research Projects Agency
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems Computer Emergency Response Teams
IIoT	Industrial Internet of Things
IMIP	Industrial Modernization Incentives Program
ICT	information and Communications Technology
Industry 4.0	Manufacturing environment that uses cyber-physical systems, Internet of Things, and cognitive computing to monitor the physical processes of the factory
IoT	Internet of Things
ISAC	Information Sharing and Analysis Center
ISAO	Information and Sharing Organizations
IT	Information Technology
MET	Manufacturing Environment Team (a CFAM JWG team)
MIBP	Manufacturing and Industrial Base Policy
NCCIC	National Cybersecurity and Communications Integration Center
NCWF	National Initiative for Cybersecurity Education Cybersecurity Workforce Framework



NDAA	National Defense Authorization Act
NDIA	National Defense Industrial Association
NGDP	Next Generation Data Protection
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Internal / Interagency Report
NCCoE	National Cybersecurity Center of Excellence
NNMI	National Network for Manufacturing Innovation
NNPD	National Protection & Programs Directorate
ODASD(R&E)	Office of the Deputy Assistant Secretary of Defense (Research and Engineering)
ODASD(L&MR)	Office of the Deputy Assistant Secretary of Defense (Logistics and Materiel Readiness)
OEM	Original Equipment Manufacturers
OSD	Office of the Secretary of Defense
OIP	Office of Infrastructure Protection
OT	Operational Technology
OTA	Other Transactions Arrangements
PaaS	Platform as a Service
PPI	Policy, Plans, and Impacts (a CFAM JWG team)
PPP	Program Protection Plan
R&D	Research and Development
RFI	Request for Information
RMF	Risk Management Framework
S&MEs	Small and Mid-Sized Enterprises
SCADA	Supervisory Control and Data Acquisition
SBIR	Small Business Innovative Research
SECaaS	Security as a Service
SERC	Systems Engineering Research Center
TS	Technology Solutions (a CFAM JWG Team)
TTP	Tactics, Techniques, and Procedures



UARC	University Affiliated Research Center
USD(AT&L)	Undersecretary of Defense (Acquisition, Technology & Logistics)
USB	Universal Serial Bus
VR	Virtual Reality